DRAFT REGULATORY GUIDE

C-006 (REV. 1) (E)

SAFETY ANALYSIS OF CANDU NUCLEAR POWER PLANTS

Issued for public comments by the
Atomic Energy Control Board
September 1999

Atomic Energy Control Board | Commission de contrôle de l'énergie atomique

Canada

DRAFT REGULATORY GUIDE

Safety Analysis of CANDU Nuclear Power Plants
(C-006, Rev. 1) (E)

draft

Issued for public comments by the
Atomic Energy Control Board
September 1999

AECB Regulatory Documents

The Atomic Energy Control Board (AECB) operates within a legal framework that includes law and supporting regulatory documents. Law includes such legally enforceable instruments as acts, regulations, licences and directives. Regulatory documents such as policies, standards, guides, notices, procedures and information documents support and provide further information on these legally enforceable instruments. Together, law and regulatory documents form the framework for the regulatory activities of the AECB.

The main classes of regulatory documents developed by the AECB are:

- **Regulatory Policy:** a document that describes the philosophy, principles and fundamental factors used by the AECB in its regulatory program.
- **Regulatory Standard:** a document that is suitable for use in compliance assessment and describes rules, characteristics or practices which the AECB accepts as meeting the regulatory requirements.
- **Regulatory Guide:** a document that provides guidance or describes characteristics or practices that the AECB recommends for meeting regulatory requirements or improving administrative effectiveness.
- **Regulatory Notice:** a document that provides case-specific guidance or information to alert licensees and others about significant health, safety or compliance issues that should be acted upon in a timely manner.
- **Regulatory Procedure:** a document that describes work processes that the AECB follows to administer the regulatory requirements for which it is responsible.

Document types such as regulatory policies, standards, guides, notices and procedures do not create legally enforceable requirements. They support regulatory requirements found in regulations, licences and other legally enforceable instruments. However, where appropriate, a regulatory document may be made into a legally enforceable requirement by incorporation in an AECB regulation, a licence or other legally enforceable instrument made pursuant to the *Atomic Energy Control Act*.

101-02853/

DRAFT REGULATORY GUIDE

Safety Analysis of CANDU Nuclear Power Plants

C-006 (Rev. 1)(E)

September 1999

NOTICE

On March 20, 1997, Bill C-23, the Nuclear Safety and Control Act (NSC Act), received Royal Assent. New regulations that are derived from this Act will become law and replace the existing regulations. Regulatory Guide C-006 (Rev. 1) references the NSC Act and new regulations, which will come into force on a date to be fixed by order of the Governor in Council.

Preface

Consultative Document C–006 (Rev. 1) supersedes Consultative Document C–6, which was issued for comments in June 1980. In June 1983, the Atomic Energy Control Board (AECB) applied C–6, on a trial basis, to the licensing of the Darlington Nuclear Generating Station, C–006 (Rev. 1) consolidates lessons learned from the trial application as well as all comments received since then.

Consultative Document C–006 (Rev.1) is being reissued to provide an opportunity for further public review before being designated as an AECB Regulatory Guide. The content of this draft regulatory guide reflects the philosophy of the new Nuclear Safety and Control Act (NSC Act) and its proposed regulations which are expected to come into force in 2000. Comments are encouraged and should be directed to the address below before December 15, 1999. All comments should be provided in writing, referencing file number 1–8–8–6.

Unless otherwise requested, a copy of all comments received will be placed in the AECB Library, in Ottawa.

Document availability

The document can be viewed on the AECB Internet website at www.aecb-ccea.gc.ca. Copies of C-006 (Rev. 1) may be ordered in English or French using the contact information below.

Operations Assistant
Corporate Documents Section
Atomic Energy Control Board
P.O. Box 1046, Station B
Ottawa ON K1P 5S9
Telephone: (613) 996-9505
Facsimile: (613) 995–5086
E-mail: reg@atomcon.gc.ca

Contents

About This Regulatory Guide viii

Purpose viii

Scope viii

Who Should Read This Guide ix

How This Guide Is Organized ix

Approach Used in the Guide x

Related Documents x

1. General Guidance and Procedures 1

1.1 Reporting 1

1.1.1 General Guidance 1

1.1.2 Computer Codes and Data 1

1.1.3 Verification 1

1.1.4 Quality Assurance Program 1

1.1.5 Non-conformance 2

1.2 Revision of Safety Analysis 2

1.2.1 Safety Reviews 2

1.2.2 Revision and Integration 2

1.3 Quality Assurance 2

1.3.1 Quality Assurance Program 2

1.3.2 Organizational Factors 3

1.3.3 Safety Analysis Procedures 3

1.3.4 Safety Analysis Integration 4
1.3.5 Quality Assurance Procedures 4
1.3.6 Verification Procedures 4
1.3.7 Reporting Procedures 5
1.4 Unresolved Safety Analysis Issues 5
1.4.1 Identification of Issues and Submitting Program Reports 5
1.5 Overview of the Safety Analysis Process 5
2. Systematic Review of the Nuclear Power Plant **9**
2.1 Identify Documentation 9
2.1.1 Introduction and Examples 9
2.2 Review Identified Documentation 10
2.2.1 Introduction 10
2.2.2 Plant State Parameters 10
2.2.3 Plant States Beyond Allowable Limits 12
2.2.4 Safety-Related Items 13
2.2.5 Failure Modes 15
2.2.6 Common Cause Events 17
2.2.7 Event Combinations 18
2.2.8 Event Sequences 19
2.2.9 Weather 19
2.2.10 Dependencies 19
2.2.11 Failure Sequences 21
3. Treatment of Common Cause Events **23**

3.1 Recommended Methodology 23
3.1.1 Hazard Assessment 23
3.1.2 Mitigating Systems 23
3.1.3 Qualified Components 24
3.1.4 Operating Procedures 24
3.1.5 Release and Dose Estimates 24
3.2 Alternative Methodology 24
4. Treatment of Failure Sequences **25**
4.1 Classification of Events 25
4.1.1 Initiating Events 25
4.1.2 Event Combinations 28
4.1.3 Event Combinations with Common Cause Events 29
4.1.4 Event Sequences 29
4.1.5 Shutdown Systems 32
4.1.6 Independence of the ECCS 33
4.1.7 Single Failure in Special Safety Systems 33
4.1.8 Single Operator Error 33
4.1.9 Worst Plant State 33
4.1.10 Failure Sequences Involving Partial Failure 34
4.1.11 Subdivision of Failure Modes 34
4.1.12 Worst Piping and Header Failure 34
4.1.13 Vessel Failure 35

4.1.14 Weather 35
4.1.15 Dependencies 35
4.1.16 Dependencies Between Events 36
4.1.17 Cutoff 36
4.1.18 Overpressure Protection 36
4.1.19 Acceptance of Classification 36
4.2 Analysis of Failure Sequences 36
4.2.1 Documentation 36
4.2.2 Failure Sequence Groups 37
4.2.3 Limiting Failure Sequences 37
4.2.4 Safety Related Items 37
4.2.5 Capability and Qualification of Mitigating Systems 38
4.2.6 Capability of Components that are Not Qualified 38
4.2.7 Minimum Allowable Performance Standards 38
4.2.8 Coverage of Actuation Parameters 38
4.2.9 Operator Action 38
4.2.10 Duration of Analysis 40
4.2.11 Reactor Physics 40
4.2.12 Heat Transfer 40
4.2.13 Integrity of Fuel, Pressure Retaining Components, and Structures 41
4.2.14 Release of Radioactive Materials 41
4.2.15 Doses for the Duration of the Release 42

4.2.16 Derived Acceptance Criteria 43
4.2.17 Associated Regulatory Requirements 44
4.2.18 Validity of the Analysis 44
4.2.19 Safety Margins 45
4.2.20 Mathematical Models and Calculational Methods 45
4.2.21 Conservative Assumptions 45
4.2.22 Verification 48
4.2.23 Validation 48
4.2.24 Commissioning Tests 49
4.2.25 Data 49
4.2.26 Intermediate Results 49
4.2.27 Acceptance Criteria 49
5. Probabilistic Safety Assessment 61
5.1 Scope 61
5.2 Use of the PSA in Analysis 61
Glossary 65
Appendix A: Probabilistic Technique for Classification of Events A.1
Appendix B: Limiting Events B.1

About This Regulatory Guide

Purpose

The *Guide for the Safety Analysis of CANDU Nuclear Power Plants* provides guidelines for developing a safety analysis report for CANDU nuclear power facilities. It is intended to help licence applicants meet the expectations of the AECB regarding safety analyses, which licence applicants are required to submit to the AECB in accordance with the regulations.

The guidelines provided in this document are not mandatory. The primary responsibility for safety analysis rests with the licensees and applicants. Licensees and applicants are given latitude in deciding whether another approach would achieve an equivalent or better safety margin. In all cases, alternative approaches for safety analyses proposed by a licensee will only be accepted if they are defensible and the AECB is satisfied that the approach meets the intent of the regulations. Conformance with the guidelines will expedite the licence assessment process.

Scope

This guide applies to the safety analysis of new CANDU nuclear power plants that will be required by paragraph 6(c) of the *Class 1 Nuclear Facilities Regulations* under the *Nuclear Safety and Control Act*. Safety analyses and quality assurance activities performed under paragraph 3(1)(i) of the General Regulations and paragraphs 4(d) or 5(f) of the *Class 1 Nuclear Facilities Regulations* are outside the scope of this document, however, the practices described in this guide may be useful.

The safety analysis requirements for existing plants are outside the scope of this document, however, the practices described in this guide may be useful for their revision.

The guide covers all essential practices and acceptance criteria for safety analyses submitted in support of the licensing of a CANDU nuclear power plant. It is not a detailed safety analysis standard nor is it a template for producing a final safety analysis report, although such standards and templates should be developed by the power plant safety analysts as part of the safety analysis.

Who Should Read This Guide

This guide is aimed at:

- licensees and applicants who operate or design Class 1 nuclear facilities (CANDU nuclear power plants) – to help in the preparation of final safety analysis reports to support a licence application.
- AECB staff – to help assess the degree to which the applicant has made adequate provision for safety in the design of the facility.

How This Guide Is Organized

This guide is organized according to the following structure:

- Section 1, "General Guidance and Procedures" provides guidelines that apply to all safety analyses.
- Section 2, "Systematic Review of the Nuclear Power Plant" provides guidelines for the review of the nuclear power plant.
- Section 3, "Treatment of Common Cause Events" provides guidelines for hazard assessment of the plant in response to common cause events.
- Section 4, "Treatment of Failure Sequences" provides guidelines for classification of events and analysis of failure sequences (i.e., events other than common cause events).
- Section 5, "Probabilistic Safety Assessment" provides general information about how a Probabilistic Safety Assessment is to be used in a safety analysis.
- "Glossary" provides definitions of key terminology used in this guide.
- Appendix A, "Probabilistic Technique for Classification of Events" provides guidelines on an alternative technique for event classification.
- Appendix B, "Limiting Events" provides a methodology for identifying limiting events for plant parameters and operating procedures.

Approach Used in the Guide

This guide describes a deterministic analysis of individual event combinations; that is, the guidelines do not describe how to determine the probability of an event occurring. (The notable exception is the Probabilistic Safety Assessment, which describes the calculation of probabilities.)

By following the approach described in this guide, the safety analyst should be able to assess the adequacy of the plant's operating procedures and identify the limiting parameters of the plant, namely:

- the design parameters of the mitigating systems, and
- the operating parameters of the plant.

The guidelines are intended to assist the analyst in formulating intermediate acceptance criteria based on the current state of knowledge. The guidelines use the hypothesis that the plant in question is assumed unsafe until proven safe to a high level of confidence, with the burden of proof on the analyst. Through such an exercise, the analyst will determine whether the functional capability of the plant's design and operational procedures provide sufficient protection, and whether additional safeguards and mitigating provisions are needed.

Related Documents

For additional information related to safety analyses not covered in this guide, refer to:

- Nuclear Safety and Control Act (NSC Act)
- General Nuclear Safety and Control Regulations
- Class 1 Nuclear Facilities Regulations
- AECB, Requirements for Containment Systems for CANDU Nuclear Power Plants, Regulatory Document R-7.
- AECB, Requirements for Shutdown Systems for CANDU Nuclear Power Plants, Regulatory Document R-8.
- AECB, Requirements for Emergency Core Cooling Systems for CANDU Nuclear Power Plants, Regulatory Document R-9.
- AECB, Overpressure Protection Requirements for Primary Heat Transport Systems in CANDU Power Reactors Fitted with Two Shutdown Systems, Regulatory Document R-77.
- ICRP 68, International Commission on Radiological Protection, Dose Coefficients for Intakes of Radionuclides by Workers, 1994.
- ICRP 72, Age-Dependent Doses to Members of the Public from Intakes of Radionuclides: Part 5 - Compilation of Ingestion and Inhalation Dose Coefficients, 1996.

- Radiation Protection Bureau of Health Canada, Recommendations on Dose Coefficients for Assessing Doses from Accidental Radionuclides Releases to the Environment, 1998.
- CAN/CSA–N288.2–M91. Guidelines for Calculating Radiation Doses to the Public from a Release of Airborne Radioactive Material under Hypothetical Accident Conditions in Nuclear Reactors.
- CAN/CSA–N288.1–M87. Guidelines for Calculating Derived Release Limits for Radioactive Material in Airborne and Liquid Effluents for Normal Operation of Nuclear Facilities.
- D.G. Hurst and F.C. Boyd. Reactor Licensing and Safety Requirements, AECB–1059, June 1972.
- AECB, Regulatory Guide for Computer Programs Used in Design and Safety Analyses of Nuclear Power Plants and Research Reactors, Regulatory Guide G-149.

1. General Guidance and Procedures

This section provides guidelines that apply to all safety analyses.

1.1 Reporting

1.1.1 General Guidance

Submit to the AECB sufficient[1] verifiable information to demonstrate the extent to which the guidelines contained in this guide have been followed to meet the requirements of the NSCA, Regulations, licence conditions, and to facilitate a comprehensive, independent assessment of the safety analysis. Provide a listing of reference materials, on which the submitted information is based. Establish a format, content and schedule[2] of submissions acceptable to the AECB.

1.1.2 Computer Codes and Data

Document[3] all computer codes and their data in accordance with engineering codes and standards accepted by the AECB.

1.1.3 Verification

Provide to the AECB evidence, in the form of a written report, that the safety analysis has been verified according to procedures approved by the licensee or applicant, corrective action has been taken for all identified deficiencies, and whether the verifier concurs with the corrective action. Justify the scope of verification performed.

1.1.4 Quality Assurance Program

Submit to the AECB evidence, in the form of a written report, submitted at a frequency accepted by the AECB, that the quality assurance program is being audited and reviewed according to procedures approved by the licensee or applicant. Such evidence should demonstrate that the quality assurance program has been established and implemented effectively and that corrective action has been taken for all identified deficiencies.

1.1.5 Non-conformance

Report non-conformances to the AECB and provide justification[4].

1.2 Revision of Safety Analysis

1.2.1 Safety Reviews

Periodically, identify safety analysis deficiencies. Submit the list of deficiencies in accordance with a schedule acceptable to the AECB even when no deficiencies are found. To identify such deficiencies, conduct auditable reviews of:

- new safety standards, analytical methods, and technical and scientific research
- changes in power plant data, design, operating envelope, and operating procedures
- accumulated information on worldwide nuclear power plant commissioning and operating experience.

1.2.2 Revision and Integration

Revise the safety analysis to account for any deficiencies identified by the review. Submit the safety analysis in accordance with a schedule acceptable to the AECB. Integrate the revisions into the final safety analysis report in a timely manner as required by a licence condition[5].

1.3 Quality Assurance

1.3.1 Quality Assurance Program

(a) Establish a quality assurance program that complies with regulatory requirements, codes, standards, and acceptance criteria applicable[6] to the safety analysis. Apply the program to all safety analyses performed during the life cycle of the nuclear power plant. Submit the QA program manual to the AECB for acceptance before the start of any[7] safety analysis activity. Submit changes made to the program for acceptance.

(b) Include in the QA program:

- organizational factors
- safety analysis procedures
- safety analysis integration procedures
- quality assurance procedures
- verification procedures
- reporting procedures.

1.3.2 Organizational Factors

Document organizational factors. Outline qualifications of personnel, organizational structure, responsibilities and authority for:

- the nuclear power plant
- the safety analysis
- the interfaces between safety analysis, safety research, design, operation, and reliability analysts
- verification
- audit and review.

1.3.3 Safety Analysis Procedures

(a) Document the safety analysis procedures for:

- executing the nuclear power plant review
- classifying the events into event classes
- preparing and selecting analysis methods
- analysing the failure sequences
- validating the safety analysis
- treating common cause events
- conducting a probabilistic safety assessment
- identifying unresolved safety issues.

(b) In the procedures, cover two phases of the life of the nuclear power plant, namely:

- the safety analysis of the interim design and operating procedures at each reference design point during the various stages of the design phase, and
- updates in regulatory requirements, knowledge and experience or changes made to the design and operating procedures during the construction, commissioning and operation phases.

(c) Identify the level of rigour (for example, analysis, assessment relative to events that are more limiting, experiment, or operational experience) to be applied to the safety analysis.

1.3.4 Safety Analysis Integration

Document the safety analysis integration procedures: that is, procedures for integrating the safety analysis activities and ensuring effective communication among the designers, operators, safety analysis disciplines, the analysts within each safety analysis discipline, safety researchers, and reliability analysts.

1.3.5 Quality Assurance Procedures

Document the quality assurance procedures. These procedures include:

- determining the extent of the safety analysis quality assurance program to be applied to each task of the safety analysis activity
- planning and training
- configuration management, change control, maintaining essential records such that the analysis is scrutable, repeatable and traceable
- audit and review
- corrective action.

1.3.6 Verification Procedures

Document verification procedures to determine the extent of independent verification to be applied to each task of the safety analysis. Apply independent verification when defining the operating procedures and performance requirements of the mitigating systems. Justify the extent of independent verification performed.

1.3.7 Reporting Procedures

Include a procedure for the submission to the AECB of all key safety analysis reports.

1.4 Unresolved Safety Analysis Issues

1.4.1 Identification of Issues and Submitting Program Reports

Clearly identify all unresolved safety analysis issues[8], and submit to the AECB a schedule and plan for a research program that addresses these issues. Submit reports in accordance with a schedule acceptable to the AECB.

1.5 Overview of the Safety Analysis Process

Figure 1.1 below shows a graphical depiction of the process to be employed when conducting a safety analysis. Where applicable, the reference to the appropriate section of this guide is provided for each process.

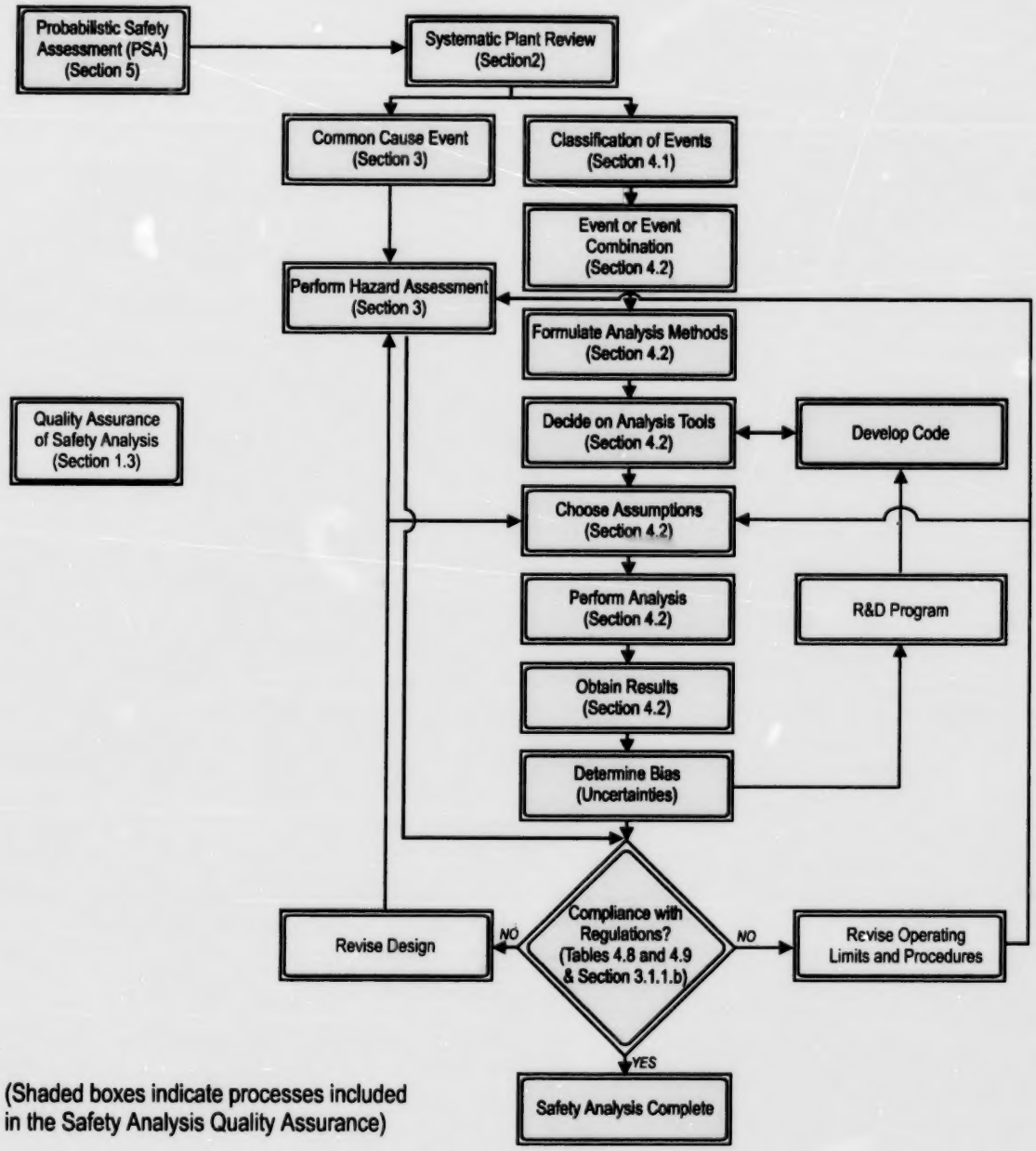
Probabilistic Safety Assessment (PSA) (Section 5)
Systematic Plant Review (Section2)
Common Cause Event (Section 3)
Classification of Events (Section 4.1)
Event or Event Combination (Section 4.2)
Perform Hazard Assessment (Section 3)
Formulate Analysis Methods (Section 4.2)
Quality Assurance of Safety Analysis (Section 1.3)
Decide on Analysis Tools (Section 4.2)
Develop Code
Choose Assumptions (Section 4.2)
Perform Analysis (Section 4.2)
R&D Program
Obtain Results (Section 4.2)
Determine Bias (Uncertainties)
Revise Design
NO
Compliance with Regulations? (Tables 4.8 and 4.9 & Section 3.1.1.b)
NO
Revise Operating Limits and Procedures
YES
Safety Analysis Complete
(Shaded boxes indicate processes included in the Safety Analysis Quality Assurance)

Figure 1.1: Safety Analysis Process

Notes

1. Throughout the guide, guidelines are provided in the form of specific items to be reported.
2. Allow sufficient time for review by the AECB.
3. The code and data documentation should include the code development and application documentation outlined in G-149, quality assurance plan, configuration management plan, training material, and data description and verification reports.
4. Justification for non-conformance should include a description of the consequences of the event with conformance. Non-conformances that have been accepted are noted in this guide.
5. R-99 sets out the reporting period for safety report revisions.
6. The requirements, codes and standards may be referenced, and procedures may be included to derive criteria.
7. This refers to licensing analysis and implies that a safety analysis organization has an existing safety analysis quality assurance program.
8. Examples of such issues include: standards for accounting for error tolerances in safety analysis, the extent of quality assurance and independent verification, qualifications of safety analysts, analysing cross-link effects and other dependencies, and Probabilistic Safety Assessment techniques for CANDU. Other examples include instances of the corrective action being unsatisfactory to the verifier, and outstanding validation of safety analysis assumptions.

2. Systematic Review of the Nuclear Power Plant

This section provides guidelines for the review of the nuclear power plant. This review entails a thorough examination of the documentation pertaining to the plant.

2.1 Identify Documentation

2.1.1 Introduction and Examples

(a) Identify the power plant's available[1] site and design documentation and operating procedures. Also identify the available documentation of root cause analysis of events in Canada and other countries[2] that utilize similar technology. Identify topics where this documentation is incomplete or does not represent the actual configuration.

(b) Examples of documentation to be identified and reviewed may include:

- meteorological databases
- seismic databases
- geological data
- hydrological databases
- design manuals
- flow sheets
- electrical diagrams
- drawings
- operating manuals
- operating policies and principles/technical specifications
- maintenance program
- equipment calibration program
- surveillance routines (panel checks, operator routines, routine test procedures, inspections)
- call-ups.

(c) The review may also use documentation used for classification of safety-related items for such purposes as quality assurance, seismicity, fire, pressure retention, or reliability.

2.2 Review Identified Documentation

2.2.1 Introduction

Perform a systematic and auditable review[3] of the power plant site, design, operating procedures, and documented experiences of other countries. Identify the following:

- plant state parameters
- plant states beyond allowable limits
- safety-related items, their functional capabilities and their failure modes
- common cause events that are events of concern
- event sequences that are events of concern
- weather scenarios
- dependencies
- failure sequences.

2.2.2 Plant State Parameters

Identify all plant states for which continued operation is allowed by the operating procedures. Include the plant state parameters listed in Table 1.1 as applicable. (Note that Table 2.1 may not be exhaustive.) Plant state parameters may be measured or calculated. Include transient plant states and their time dependencies over the life of the plant.

For each applicable plant state:

- Identify instruments used to detect the plant state and their error tolerances.
- Identify calculational methods used to determine the plant state and provide a confidence interval on their biases.

Table 2.1: Specified Plant State Parameters

- inventory of radioactive materials (fission products, tritium, activation products, fuel) in the primary and secondary coolant, and moderator
- gap inventory in the fuel
- fuel sheath defects
- leakage or bypass of valves, seals, boiler tubes, pressure tubes, and containment
- initial fuel centreline temperatures and powers
- flux shapes
- moderator poison
- core burnup: fresh, pre-equilibrium, equilibrium
- pressures, temperatures, flows, and levels
- instrument tolerances
- instrument time constants and delays
- component ageing, thermal cycles, cracking, deformation, strain, wear, and degradation (including boiler tubes and pressure tubes)
- position of valves, dampers, doors, gates, hatches, covers, plugs, gratings, switches, circuit breakers, and relays
- operating mode
- shutdown states: primary heat transport open and closed, drained and full, cold and hot, guaranteed shutdown, and critical
- shutdown heat sinks: boilers, residual heat removal system, and moderator
- start up
- power level
- power manoeuvring
- shim
- refuelling
- calibration
- testing
- maintenance
- inspection
- number of components, such as pumps and valves, operational

...continued

Table 2.1: Specified Plant State Parameters (cont.)

- number of fuel bundles and shield plugs in a channel
- number of units shut down in a multi-unit power plant
- range of allowable axial gaps between the fuel string and the shield plug in a channel
- range of allowable states of safety-related items defined by their minimum allowable performance standards (including set points)
- maximum allowable undetected flow blockage following refuelling
- when allowed by the operating procedures, effects resulting from all failure sequences, which remain after returning the nuclear power plant to normal operation

2.2.3 Plant States Beyond Allowable Limits

Identify plant states that have occurred or are anticipated to occur over the life of the plant for which action is required to return the plant to an allowed plant state. This refers to plant states that extend beyond the allowable limits of magnitude, duration, or both. Include the parameters specified in Table 2.2 as applicable. (Note that Table 2.2 may not be exhaustive.)

Table 2.2: Specified Beyond Allowable Plant State Parameters

- excessively low or high temperature (e.g., moderator)
- excessively low or high pressure (e.g., loss of containment vacuum)
- excessively low or high level
- excessively low or high flow
- excessive leak area (e.g., containment open airlock doors)
- excessively small axial gap between the fuel string and the shield plug in a channel
- excessively high activity (e.g., iodine spiking)
- excessively low or high or miscalibrated measurement (e.g., thermal power)
- miscalibrated high pressure protection
- miscalibrated high neutron flux protection
- miscalibrated high rate of increase of the logarithm of neutron flux protection
- miscalibrated boiler low level protection

2.2.4 Safety-Related Items

Include the safety-related items listed in Table 2.3, as applicable. Using the operating procedures, identify both normal and emergency operator actions.

Table 2.3: Specified Safety-Related Items

- shutdown system 1
- shutdown system 2
- emergency core cooling system
- containment system
- pressure relief valve
- automatic pump trip
- emergency heating, ventilation, and air conditioning
- Class III emergency electrical power
- emergency electrical power
- emergency compressed air
- firewater
- boiler emergency cooling system
- emergency service water system
- hydrogen mitigation systems
- residual heat removal system
- auxiliary boiler feedwater system
- auxiliary condensate system
- reactor primary coolant inventory control system
- reactor primary coolant pump gland seal circulation
- reactor primary coolant system
- reactor primary coolant purification system
- reactor regulating system
- reactor regulating system setback
- reactor regulating system stepback

...continued

Table 2.3: Specified Safety-Related Items (cont.)

- reactor secondary coolant system
- service water system
- moderator system
- moderator cover gas system
- moderator poison system
- D2O management
- reactor shield cooling
- control computer
- backup control computer
- turbine generator
- turbine overspeed protection
- annulus gas system
- compressed air
- isolation valve
- heating, ventilation, and air conditioning
- fuelling
- irradiated fuel bay cooling
- irradiated fuel bay purification
- irradiated fuel bay air purification system
- radioactive waste (gas, liquid, and solid) management system
- normal electrical power
- Class IV auto transfer
- gaseous effluent monitor
- gaseous fission product and failed fuel location
- reactor primary coolant recovery system
- moderator recovery system
- supports
- structures
- operating procedures of safety-related systems

2.2.5 Failure Modes

For each failure mode, identify how and when the failures are detected and the lost functional capability or the undesirable function performed. Include failure to perform a procedure when required and performing a procedure when inappropriate, in addition to the failure modes listed in Table 2.4.

Table 2.4: Specified Failure Modes

In general, failure includes: • failure prior to the initiating event • failure as the initiating event • failure during the mission • operator inaction • left in wrong state • placed into service under inappropriate conditions • unavailable because of being in maintenance outage • in test outage • not returned to service after maintenance • not returned to service after test • massive failure (break or buckle) • cross-link effects
For valves, dampers and doors, failure includes: • stuck closed or open • left closed or open by the operator • closes or opens spuriously prior to initiating event, as the initiating event or during the mission • failure to reopen or reclose • passing (internal or external leak) • partial opening or closing • opening or closing at the wrong speed

...continued

Table 2.4: Specified Failure Modes (cont.)

For pumps, fans, turbines and compressors, failure includes: • failure to start • failure to run • failure to stop • fails to restart • starts spuriously prior to initiating event, as the initiating event or during the mission • seizure • failure of shaft • breakup
For reactivity mechanisms, failure includes: • failure to drop • drops spuriously • failure to withdraw • drops slowly • inadvertent withdrawal • inadvertent poison dilution
For instrumentation, failure either prior to the initiating event, as the initiating event or during mission includes: • failure of output to zero • failure of output low or high • setpoint or output drifts low or high • failure not detected during diagnosis • miscalibration • constant output • noisy output

Table 2.4: Specified Failure Modes (cont.)

For electrical circuits, failure either prior to the initiating event, as the initiating event or during the mission includes:

- short or open circuit
- switch left in wrong position
- computer program malfunction
- failure of digital computer control system

For cooling systems, including ECCS, failure either prior to the initiating event, as the initiating event or during mission includes:

- failure of system piping and hoses (single and multiple, internal or external leaks)
- failure of circulation (flow)
- failure of preheating or heat removal capability (heat sink)

For the containment system, failure includes:

- deflation of airlock door seals while the other airlock door is open
- failure of automatic containment isolation logic
- failure of isolation dampers
- loss of dousing
- loss of emergency filtered air discharge
- failure of pressure relief valves
- failure of containment cooling
- failure of hydrogen control
- failure of reverse flow valves

2.2.6 Common Cause Events

Identify all credible[4] events that the plant was designed to withstand (design basis common cause events), including those specified in Table 2.5. (Note that Table 2.5 may not be exhaustive.) Quantify and justify the parameters[5] of these events. The parameters for common cause events that occur during normal operation may differ from those that occur within 30 days or the time required to restore the plant to normal operation, whichever is less, before or after another common cause event or another initiating event. Submit these parameters to the AECB for acceptance prior to proceeding to the hazard assessment (described in Section 3).

Table 2.5: Specified Common Cause Events

- fire (one fire area, flammable liquids, flammable gas clouds)
- earthquake
- tornado
- explosion
- release of toxic gases
- release of corrosive chemicals
- internal flooding
- external flooding
- extreme weather (wind, rain, hail, snow, ice, lightning, temperature, drought)
- aircraft crash
- electromagnetic interference from telecommunications equipment
- events in other reactors on the site

2.2.7 Event Combinations

Identify all credible event combinations of safety-related item failures and common cause events that may occur within 30 days after the initiating event or the time required to restore the plant to normal operation, whichever is less. Include combinations consisting of an event and a plant state that have occurred or are anticipated to occur over the life of the plant for which action is required[6] to return the plant to an allowed plant state.

2.2.8 Event Sequences

(a) Identify an event sequence for each combination of success or failure[7] of each of the mitigating provisions for each event of concern that has an initiating event that is not a common cause event. Failure of a mitigating provision includes failure to carry out a procedure when required. Identify all events with a total annual probability greater than 10^{-7}.

(b) If the AECB has given written acceptance for treating the subsystem as being independent, the event sequences need only include an event sequence for each combination of success or failure of any one of each of the subsystems of a special safety system.

(c) For each serious process failure, include an event sequence for each combination of success or failure of any one[8] of each component in each special safety system that:

- must change state, or
- is dependent on a safety support system function.

2.2.9 Weather

The duration of the weather scenarios is 30 days.

2.2.10 Dependencies

Identify dependencies, (including cross-link effects) among all combinations of plant state parameters, the bias and variance of instrument errors, bias in calculational methods, weather scenarios, initiating events, event combinations, event sequences, and failures of safety-related items, including operator actions. Include the dependencies specified in Table 2.6, as applicable. (Note that Table 2.6 may not be exhaustive.)

Table 2.6: Specified Dependencies

Type	Dependencies
Plant State	• equipment unavailable when shutdown or at low power • equipment running when shutdown or at low power • weather and power dependency on time during daily load following • iodine spike following shutdown, startup, or defuelling • high poison during startup
(Initiating) Event	• breaks for which containment isolation is blind • time available for operator action • reduced margin causing spurious failure following an event
Environmental	• equipment (including components such as fuel, fuel channels, calandria, boiler tubes, valves, pumps and the control room) fails or is inaccessible in a hostile environment (flooding, condensation, humidity, wet instrument air, corrosion, vibration, pressure, radiation, temperature, and heating by fuel, activation products, fission products, steam or a standing hydrogen flame) • boiler tubes leak or rupture when an event occurs • calandria fails when deflagration occurs
Dynamic Effects	• water hammer • impact loads • reaction forces • pipe whip and fluid jets following a pressure boundary failure • hydrodynamic loads from chugging and condensation oscillation • shock waves from hydrogen combustion, fuel channel rupture or molten fuel moderator interaction • calandria tube fails when the pressure tube fails • end fitting ejection when the pressure tube or end fitting fails • fuel ejection when the pressure tube or end fitting fails • lattice tube fails when the end fitting fails • loss of primary coolant from single or multiple fuel channels from fuelling failure • second pressure boundary break from fuel string impact when inlet break occurs

Table 2.6: Specified Dependencies (cont.)

Functional Effects	• coincidence of functional requirements causing overload • changed net positive suction head • increased load demand on an electrical bus • accelerated flow across valves • filter overloading • increased pressure or stresses • reduced margin causing spurious actuation following an event
Common Cause Effects	• precursors (for example, a common deficiency in: design, fabrication, installation, commissioning, or operating procedures such as maintenance or commonalities in the calibration procedures for both shutdown systems) contributing to failure of the mitigating system and either the initiating event, or other mitigating systems • the use of common personnel (designer, maintainer, analyst)
Operator Actions	• actions resulting from diagnosis, using operating procedures when the indications are ambiguous

2.2.11 Failure Sequences

Derive the failure sequences by defining each combination of plant state and weather scenario for each event sequence. Account for dependencies.

Notes

1. Maintaining nuclear power plant documentation is outside the scope of this guide.

2. Information on events at other nuclear facilities may be found in the Incident Reporting System of the International Atomic Energy Agency (IAEA), Organization for Economic Co-operation and Development (OECD), and Nuclear Energy Agency (NEA).

3. The review should conform with internationally recognized standards. Use a failure modes and effects analysis (FMEA) to satisfy some of the elements of the systematic review. Use probabilistic safety assessment (see Section 5). The assessment may complement, augment or support an FMEA particularly to cope with initiating events linked mainly to common cause or multiple failures. This is to confirm, for example, reliability, separation, and diversification of heat sinks.

4. The definition of individual design basis common cause events is outside the scope of this document. They are not intended to be of as high a probability as Class 1 events or as low as a Class 5 event. Credible design basis common cause events will be less severe when occurring within a period following an event.

5. For example, a design-basis tornado will be quantified in terms of tornado parameters—wind speed, vortex translational speed, radius of maximum tangential wind speed, and maximum atmospheric pressure drop—and tornado-generated missiles.

6. A plant state that has occurred or is anticipated over the life of the plant for which operator action is required to return the plant to an allowed state is treated as an event consisting of a failure of the configuration control of the plant.

7. Failure of mitigating provisions includes prior failures. As such, event sequences include some event combinations (consisting of a prior failure of a mitigating provision and a subsequent initiating event). They can also be interpreted as including some low probability plant states at the time of the initiating event.

8. The analysis of cross-link effects and review of the operating procedures should determine whether other components should not be credited.

3. Treatment of Common Cause Events

This section describes guidelines for performing a hazard assessment in response to common cause events identified in the systematic review of the power plant (see Section 2).

3.1 Recommended Methodology

3.1.1 Hazard Assessment

(a) A hazard assessment consists of a systematic review of the power plant to demonstrate that:

- the plant design incorporates sufficient mitigating systems that are qualified to survive and function during and/or following each common cause event
- operating staff are equipped to carry out essential actions
- actions of operating staff are practicable.

(b) Demonstrate that the qualified systems meet the safety criteria:

- able to bring the plant to a safe shutdown state
- the integrity of the fuel in the reactor core is maintained
- the integrity of the reactor primary coolant boundary and containment are maintained to the extent that an event of concern does not occur.

3.1.2 Mitigating Systems

(a) Identify all mitigating systems (including structures and operator actions) credited during and following the event.

(b) **Note:** Only qualified mitigating systems are credited. All non-qualified safety-related systems should be assumed to fail except in cases where continued operation of these systems would result in more severe consequences. Exceptions can be made if justification is provided to support the assumption that non-qualified systems will not fail.

3.1.3 Qualified Components

Identify each qualified component and the events for which each is qualified.

3.1.4 Operating Procedures

For each event, identify plant or operating procedure parameters for which the event is limiting. Identify the corresponding safety criteria. (See Appendix B for more information).

3.1.5 Release and Dose Estimates

Estimate airborne and waterborne releases of radioactive materials and the operator dose for essential actions during and following the common cause event.

3.2 Alternative Methodology

An alternative to using a hazard assessment is to quantify and justify five sets of parameters for the event. One set of parameters pertains to each event class (see Appendix A).

4. Treatment of Failure Sequences

This section provides guidelines for classification of events and analysis of failure sequences (i.e., events other than common cause events).

4.1 Classification of Events

This subsection describes the deterministic method for classification of events and event combinations. As an alternative to the classification scheme described here, the guidance described in Appendix A may also be used to classify failure sequences.

4.1.1 Initiating Events

Classifications of initiating events are given in Table 4.1. (Note that Table 4.1 may not be exhaustive.) Classifications of initiating events that are not specified in Table 4.1 are given in Table 4.2. Initiating events in Table 4.2 apply only to systems operating[1] under design conditions.

Table 4.1: Classification of Specified Initiating Events

Class 1 Failures
Failure of: • dual computer control • reactor power control • boiler pressure control • boiler inventory control • de-aerator inventory control • primary coolant pressure control • primary coolant inventory control • residual heat removal system temperature control • moderator inventory control • moderator temperature control • compressed air (instrument or service)

...continued

Table 4.1: Classification of Specified Initiating Events (cont.)

- service water flow
- seals or valves, causing a loss of service water
- normal electrical power
- heating, ventilation, or air conditioning
- pressure relief valve in a vacuum containment system
- turbine generator load rejection or control
- condenser vacuum
- normal boiler feedwater flow
- steam line isolation valve
- piping, causing a very small loss of reactor primary coolant
- seals or valve, causing a loss or reactor primary coolant
- seals or valve, causing a loss of reactor secondary coolant
- boiler tube
- pressure tube of any fuel channel assembly
- primary pressure relief valve(s)
- primary system loop interconnect valve or pressurizer connection valve
- primary coolant purification system
- residual heat removal system (excluding piping failures other than a heat exchanger tube)
- moderator system (excluding piping failures other than a heat exchanger tube)
- seals or valve, causing a loss of moderator water
- reactor shield cooling system (excluding piping failures other than a heat exchanger tube)
- moderator cover gas system
- D_2O management
- fuelling machine to reinstall the fuel channel closure plug
- cooling system of fuelling machine
- radioactive waste (gas, liquid, and solid) management system(s)
- irradiated fuel bay cooling, purification, or ventilation systems

...continued

Table 4.1: Classification of Specified Initiating Events (cont.)

- inadvertent ECCS actuation
- inadvertent containment dousing
- fuel damage during transfer of the fuel from the reactor core to the irradiated fuel bay
- fuel damage in the irradiated fuel bay
- plant state beyond allowable limits
- operator performs a single manipulation of a procedure when not appropriate

Class 2 Failures

Failure of:

- piping, causing a loss of service water
- piping, causing a loss of reactor secondary coolant
- piping, causing a small loss of reactor primary coolant
- end fitting of any fuel channel assembly
- residual heat removal system isolation valves
- ECCS isolation valves
- boiler primary head divider
- reactor primary coolant pump shaft
- piping or calandria tube, causing a loss of moderator
- piping, causing a loss of reactor shield coolant
- fuelling machine pressure boundary
- flow blockage in a fuel channel
- seizure of a reactor primary coolant pump

Class 3 Failures

Failure of:

- piping, causing a large loss of reactor primary coolant
- large number of boiler tubes
- end fittings of many reactor-fuel-channel assemblies
- end fitting of any fuel-channel assembly with consequential failure of its lattice-tube
- components causing backflow to ECCS

Table 4.1: Classification of Specified Initiating Events (cont.)

Class 5 Failures of Extremely Low Probability*

• turbine breakup • drop of a large load on the reactivity mechanism deck • failure of a boiler support • massive mechanical failure of a reactor-primary-coolant-pump component • massive (full-length) failure of a reactor header • massive failure of the station-service-water intake tunnel or discharge duct

* Unless justification, subject to acceptance by the AECB, is given to demonstrate that the probability of these events is sufficiently low, the consequences of the events shall be determined.

Table 4.2: Classification of Initiating Events

Class Number	Failure Description
Class 1	• failure of an active system
Class 2	• failure of non-nuclear standard passive component • failure of one of many similar nuclear standard passive components
Class 3	• failure of a nuclear standard passive component

4.1.2 Event Combinations

Table 4.3 provides the classifications of event combinations of two events. Such events include any common cause events classified into the five event classes. Plant states that have occurred or are anticipated to occur over the life of the plant, for which action is required to return the plant to an allowed plant state, are treated as event Class 1 single failures. A second event can occur simultaneously with, or within 30 days of, the first event. Such event combinations are also classified using this table if the duration of the first event is sufficiently long to still be occurring when the second event occurs. In the case of triple events, use the guidelines in Appendix A to classify the event combination.

Table 4.3: Classification of Event Combinations

Class Number	Failure Description
Class 4	• Class 1 event + Class 1 event four or more days later

Class 5	• Class 3 event + Class 1 event four or more days later • Class 2 event + Class 2 event four or more days later • Class 2 event + Class 1 event ten or more hours later • Class 1 event + Class 3 event four or more days later • Class 1 event + Class 2 event ten or more hours later • Class 1 event + Class 1 event one or more hours later

+ means accompanied by

4.1.3 Event Combinations with Common Cause Events

If a common cause event is treated by a hazard assessment, the event combinations can also be treated using a hazard assessment (as described in Section 3) or the event can be classified as an event Class 5. This applies to event combinations that have one common cause event as the initiating event, one common cause event as the second event, or two common cause events.

4.1.4 Event Sequences

(a) Classification of event sequences are provided in Table 4.4. Classification of mitigating systems is provided in Table 4.5. Failures of mitigating systems in Table 4.5 apply only to systems that are credited. Do not credit systems that are not classified in this table to change state and assume them to be in their worst allowable state. The failure of a mitigating system specified in Table 4.5 does not have to be considered when the mitigating system does not need to change state to mitigate the consequences of an event.

(b) The failure of a mitigating system in Table 4.4 means that the mitigating system failed to respond to the event of concern. Pipe breaks and other passive-component or structural failures are excluded; such failures are considered to be initiating events, and are included as a combination of initiating events (as are mission failures of active components of mitigating systems).

Table 4.4: Classification of Event Sequences

Class Number	Event Sequence
Class 2 Event Sequences	• Class 1 event + failure of a mitigating process system to respond
Class 3 Event Sequences	• Class 2 event + failure of a mitigating process system to respond • Class 1 event + failure of a standby emergency system • Class 1 event + single failure in a special safety system • Class 1 event + single operator error
Class 4 Event Sequences	• Class 3 event + failure of a mitigating process system to respond • Class 2 event + failure of a standby emergency system • Class 2 event + single failure in a special safety system • Class 2 event + single operator error • Class 1 event + failure of a special safety system
Class 5 Event Sequences	• Class 3 event + failure of a standby emergency system • Class 3 event + single failure in a special safety system • Class 3 event + single operator error • Class 4 event + failure of a mitigating process system to respond • Class 4 event + single failure in a special safety system • Class 4 event + single operator error • Class 2 event + failure of a special safety system • Turbine generator load rejection + failure of turbine overspeed protection • Class 3 event + failure of a special safety system

+ means accompanied by

Table 4.5: Classification of Mitigating Systems

System Type	Mitigating System

Special Safety Systems	• shutdown system 1 • shutdown system 2 • emergency core cooling system (ECCS) • containment system
Standby Emergency Systems[2]	• pressure relief valve • automatic pump trip • emergency heating, ventilation, and air conditioning • Class III emergency electrical power • emergency electrical power • emergency compressed air • firewater • boiler emergency cooling system • emergency service water system
Mitigating Process Systems	• auxiliary boiler feedwater system • residual heat removal system • reactor primary coolant recovery system • reactor primary coolant inventory control system • moderator system • moderator poison system • isolation valve • irradiated fuel bay purification

...continued

Table 4.5: Classification of Mitigating Systems (cont.)

Mitigating Process Systems	• irradiated fuel bay air purification system • radioactive off gas management system • normal electrical power • turbine runback • annulus gas • gaseous effluent monitor • gaseous fission product monitor • failed fuel locator

4.1.5 Shutdown Systems

(a) Event sequences are classified by assuming the action of the less effective shutdown system prevents the more effective shutdown system from acting.

(b) Take credit only for the less effective of two of the less effective shutdown system's diverse[3] trip parameters. One parameter is permitted for overpower protection, fast loss of reactivity control from low power, loss of secondary coolant inventory, and overpressure protection[4] (see also document R-77). In these cases, acceptable single parameters are high neutron flux, high rate of increase of the logarithm of neutron flux, boiler low level, and high pressure respectively. However, analyse miscalibration of these trip parameters as a Class 4 or 5 event combination, treating the miscalibration as a Class 1 event.

(c) Demonstrate the effectiveness of each shutdown system for the inaction, partial action, and normal functioning of any mitigating systems[5] (including the other special safety systems) that supplement or degrade the shutdown system's negative reactivity insertion. Classify inaction and partial action of the mitigating system in the same manner as event sequences accompanied by a mitigating system failure.

4.1.6 Independence of the ECCS

Demonstrate the effectiveness of the ECCS for the inaction, partial action, and normal functioning of any mitigating systems[6] (including the other special safety systems) that supplement or degrade the cooling capability of the ECCS. Classify inaction and partial action of the mitigating system in the same manner as event sequences that have a mitigating system failure.

4.1.7 Single Failure in Special Safety Systems

Classify event sequences that have a single failure in one or more special safety systems in the event class numbered two higher[7] than the event class that has no single failure in any of the special safety systems. This applies to event sequences with no single failure in any of the special safety systems that are in event Classes 1 through 3. In the case of event sequences with no single failure in any of the special safety systems in event Class 4, classify the event sequences with a single failure in one or more special safety systems in event Class 5 (i.e., only one class higher instead of two). Assume untested components have failed.

4.1.8 Single Operator Error

Classify event sequences having a single operator error of one manipulation in the event class numbered two higher than the event class with no errors in any of the operator actions or sequence of actions. (Treat operator omission as contributing to the unavailability of the affected mitigating system.) This applies to event sequences with no operator errors that are in event Classes 1 through 3. In the case of event sequences with no operator errors in event Class 4, classify the event sequences with an operator error in event Class 5.

4.1.9 Worst Plant State

(a) Classify a failure sequence in the same event class as that of the event sequence from which the failure sequence was derived when:

- a failure sequence occurs from a plant state for which the operating procedures allow continued operation;
- a failure sequence originates from a transient plant state[8];

- a failure sequence starts from a plant state that corresponds to the tolerance[9] for instrument error and the allowance[10] for bias in the calculational method used to determine the plant state.

(b) Do not treat allowable nuclear power plant states as random variables.

(c) Analyse the worst[11] plant state in the operating envelope (including allowances for tolerances and delays for safety-related systems such as instruments) for which the operating procedures allow continued normal operation with respect to each of the safety analysis acceptance criteria. Do not subdivide failure sequences for the purposes of placing a specific failure sequence that has an allowed plant state with an anticipated low probability[12], into a higher numbered event class.

4.1.10 Failure Sequences Involving Partial Failure

Incorporate the partial and total failures of the safety-related systems in the analysis of each failure sequence. Where only the worst case[13] is analysed, give the basis on which the partial failure is chosen.

4.1.11 Subdivision of Failure Modes

Do not subdivide failure sequences for the purposes of placing a specific failure that results in the same loss of, or undesirable, function in a higher numbered event class.

4.1.12 Worst Piping and Header Failure

(a) Consider both circumferential and longitudinal failures at any location in a system. In piping and header failure analysis:

- For circumferential failures, analyse a discharge area up to, and including, twice the cross-sectional area of the piping or header.
- Consider failures resulting from longitudinal breaks and justify the maximum postulated break size.
- Perform an analysis to determine the break location, size, and orientation that are worst[14] for each of the safety analysis requirements, using a conservative break model.

(b) Analyse such failures even if acceptance has been given by AECB to allow leak- before-break analysis, detection, and response in lieu of piping restraints.

4.1.13 Vessel Failure

(a) Include massive failure of each pressure vessel in event Class 5 unless it can be demonstrated that such failure is sufficiently unlikely. If this exemption is to be achieved:

i. design, fabricate, install, and operate in compliance with the nuclear requirements of the applicable engineering code and other requirements as the AECB may deem appropriate;

ii. the vessel is not a header;

iii. undertake an in-service inspection program acceptable to the AECB;

iv. a detectable leak will occur at normal operating pressure sufficiently well in advance of the critical crack length being reached that a break will not occur; and

v. make available reliable systems to detect the presence of a leak acceptable by the AECB; develop appropriate operating procedures describing action to be taken following detection of a leak.

(b) **Note:** Items d) and e) do not apply if acceptance is given by the AECB.

4.1.14 Weather

Classify a failure sequence that occurs from a weather scenario that results in a consequence that is not exceeded a large proportion[15] of the time in the same event class as that of the event sequence from which the failure sequence was derived.

4.1.15 Dependencies

Classify a failure sequence with dependencies in the same event class as that of the event sequence from which it was derived.

4.1.16 Dependencies Between Events

If an event in the event sequence is dependent on another event in the event sequence, classify the failure sequence in the same class as an event sequence without the event that is dependent on the other.

4.1.17 Cutoff

Subject to written acceptance by the AECB, classification and analysis of an event with a total annual probability less than 10^{-6} is normally[16] not required[17].

4.1.18 Overpressure Protection

For power plants for which Regulatory Document R–77 applies, perform a separate classification of all events that result in primary heat transport system overpressure, in accordance with R–77[18].

4.1.19 Acceptance of Classification

Obtain acceptance from the AECB for classification of individual failure sequences on a case-by-case basis before submitting an analysis of the failure sequences.

4.2 Analysis of Failure Sequences

This subsection provides guidelines for performing an analysis of failure sequences.

4.2.1 Documentation

(a) For each limiting failure sequence, identify available documentation pertaining to:

- quality assurance requirements
- analysis standards and procedures
- mathematical models
- calculational methods
- experimental and analytical support.

(b) Make note of the grouping of non-limiting failure sequences, failure modes, plant states, credits for mitigating system and operator actions, duration of the analysis, analysis disciplines used, error tolerances, safety margins, and acceptance criteria.

4.2.2 Failure Sequence Groups

For each event class, identify groups of failure sequences, grouped according to similar plant response (mitigating system demand, credited operating procedures, and mitigating system and operating procedure success criteria) when weather, initial plant state, and cross-link dependencies are accounted for. For each failure sequence group, identify the credited operating procedures and the mitigating systems that respond to the transient and their success criteria.

4.2.3 Limiting Failure Sequences

Identify and analyse the variables with significant transients or uncertainties for the limiting failure sequence(s) for each operating procedure, mitigating design feature, and mitigating system performance requirement. For each requirement provide justification as to:

- why other failure sequence groups are not limiting
- why other failure sequences in the limiting failure sequence group(s) are not limiting
- why other transient variables are not analysed in detail.

4.2.4 Safety Related Items

In the analysis:

- identify the credited mitigating items
- identify the cross-link effects of the failure sequence
- determine the cross-link effects on safety-related items
- define the operating procedures[19], and performance and reliability requirements of each credited mitigating system.

4.2.5 Capability and Qualification of Mitigating Systems

Only credit the operation of mitigating systems that are designed or shown capable to meet the intended function[20] and are qualified to withstand all cross-link effects[21] arising from the failure sequence[22].

4.2.6 Capability of Components that are Not Qualified

If operation of components that are not qualified results in a worse condition, assume that such components are functioning normally.

4.2.7 Minimum Allowable Performance Standards

Only credit mitigating provisions to their minimum allowable performance standards[23] . Assume that mitigating provisions that are outside their minimum allowable performance standards have failed.

4.2.8 Coverage of Actuation Parameters

For each special safety system, analyse the extent of coverage of the actuation parameters for all plant states and failure sequences.

4.2.9 Operator Action

(a) Identify the specific operator's actions required to mitigate the consequences and the period of time required for such actions. Specifically, identify:

- the operating procedures for diagnosis, action, verification of successful action, and any remedial actions for recovery from an operator error
- the time required from occurrence of the initiating event to the indication to the operator
- the time to carry out the diagnosis
- time required to perform the action
- the time for the safety-related function to complete
- the time for indication that the safety-related function has completed

- the time required to verify that the action has been completed correctly
- the time required to complete the recovery from an error
- the supporting evidence for these times
- specific operator training necessary
- operator qualifications required for diagnosis, action, and verification
- any additional support personnel and equipment required
- diagnostic instrumentation, its qualification, and range
- verifying instrumentation, its qualification, and range
- ingress and egress paths
- environmental conditions
- credible errors in performance of the operator's actions.

(b) Assess and account for the time required for the operator to detect, completely diagnose, and carry out the required actions.

(c) Credit operator actions only if the power plant has operating procedures that identify the necessary actions, operator training, and reliable instrumentation designed to provide clear and unambiguous indication of the need to take action. The procedures shall be clear, well-defined, and readily available.

(d) Following the first clear and unambiguous indication of the necessity for operator actions, such actions may be credited no sooner than:

- 15 minutes for actions in the main control room, and
- 30 minutes for actions outside the main control room.

(e) If it is necessary to wear protective clothing to carry out the required actions, add an extra allowance equal to the time required to put on the protective clothing and the additional time required to carry out the actions while wearing protective clothing.

(f) To claim an indication as unambiguous, submit evidence to show that the indication is clear, requires no interpretation, and that multiple causes do not yield the same indication. Consider, but do not credit, operator actions taken before the minimum times allowed in the safety

analysis when demonstrating ambiguity for subsequent operator actions. Analyses using a full range of plant states, failure modes, and best estimate assumptions, may be necessary to demonstrate that the indication for corrective action is unambiguous.

4.2.10 Duration of Analysis

Perform the analysis for the period from the initiating event:

- until the power plant has returned to normal operation, or
- until the power plant has achieved a safe shutdown state, or
- until 30 days[24], if the release rate requirements of a safe shutdown state cannot be met.

4.2.11 Reactor Physics

In the analysis:

- identify the initial reactor state[25]
- determine the initial neutron flux, fluence, and power distributions in the reactor
- identify all input assumptions[26]
- calculate changes in:
  - reactor state[27]
  - detector outputs
  - reactivity
  - neutron flux and power distributions.

4.2.12 Heat Transfer

In the analysis:

- identify and quantify the power plant heat sources[28]
- identify primary heat sinks
- identify the heat transfer routes and modes from each of the heat sources to the ultimate heat sink[29]
- calculate, for each of the heat transfer routes and modes, the heat transferred as a function of time.

4.2.13 Integrity of Fuel, Pressure Retaining Components, and Structures

In the analysis:

- identify and account for normal and accident loads[30] including time dependent loads, residual loads, velocity loads, spatial loads, local and nearest neighbour loads
- calculate the effects of normal operation and the accident on material properties[31] and integrity limits
- identify and justify the assumed defect characteristics
- identify the inspection effectiveness and results
- calculate elastic and permanent deformation, stress intensity factors, expansion, shear, dissipation, motion, oscillation, waves, displacement path, diffusion, closure and opening of gaps, fatigue, and cracking
- identify the failure mechanisms
- calculate the probability of, or margin to, failure for each failure mechanism
- identify the time period of validity as well as any monitoring and ageing management practices assumed.

4.2.14 Release of Radioactive Materials

In the analysis:

- identify and quantify the radioactive materials[32] that have the potential for release
- identify, for each of these radioactive materials[33], the credited holdup volumes and barriers to release, the release pathways for each barrier, and their transport processes
- calculate, for each pathway, the release of radioactive materials from each barrier as a function of time[34] including the release from containment[35] of each group of similar radioactive materials at intervals of 1 hour, 10 hours, 4 days, and 30 days after the initiating event
- calculate the radiation fields and heating of the components and structures from the radioactive materials
- calculate the doses to the operators[36]
- calculate the atmospheric dispersion and ground deposition of the radioactive materials

- calculate the release of liquid effluent.

4.2.15 Doses for the Duration of the Release[37]

(a) Calculate[38] the dose to a hypothetical, most-exposed member of the public who is an average member of the critical group for which the radiological consequences of the release are most severe at or beyond the site boundary. Include contributions from external radiation, inhaled radioactive materials, and skin absorption of tritium using a conservative weather scenario. (A conservative weather scenario is any scenario from the upper decile of weather scenarios, ranked according to dose.) Include the external and internal doses from cloud and ground deposits, and assume no intervention in the form of decontamination or evacuation. Intervention against ingestion of radioactive materials and natural removal processes may be assumed. Repeat the dose calculation for the periods: 1 hour, 10 hours, 4 days, and 30 days after the initiating event.

(b) For the period starting 30 days after the initiating event, calculate[39] the annual dose[40] to the most-exposed member of the public who is an average member of the critical group for which the radiological consequences of the release are most severe.

Account for the contributions from all pathways including the doses committed from the 30-day release period, external radiation, inhaled radioactive materials, ingested radioactive materials, and skin absorption. Identify the dominant radioactive materials and pathways. Average the dose for weather scenarios weighted by their probability. Account for the effects on the dose of continued normal use of land and water. Assume no intervention in the form of decontamination or evacuation. Natural removal processes may be assumed.

(c) Calculate the collective dose[41] to the existing population for the periods: 1 hour, 10 hours, 4 days, 30 days, and one year after the initiating event.

4.2.16 Derived Acceptance Criteria[42]

Identify the mathematical models, calculational methods, and correlations used and their range of experimental support, assumptions (e.g., integrity of structures and components) and conditions of applicability. Identify any other constraints used to show that the dose and release limits are met. Add these constraints to Table 4.9 and show that, within a high probability[43], the requirements and limits are met. Include the limits in Table 4.6 as appropriate. (Note that Table 4.6 is not exhaustive.)

Table 4.6: Criteria Derived from Modelling Assumptions

- service level limits for containment penetrations
- avoidance of consequential boiler tube failure
- boiler tubes, fuel, and fuel channels remain fit for service
- calandria below positive design pressure
- secondary coolant below positive design pressure
- avoidance of consequential damage to in-core components
- avoidance of consequential pressure tube strain at high coolant pressure
- avoidance of consequential calandria tube dryout at high coolant pressure or when the fuel is melted or liquified
- avoidance of consequential pressure tube failure
- limit the extent, severity, and duration of fuel sheath dryout, fuel bowing, and pressure tube heating at high power for times in excess of the fuel thermal time constant
- avoidance of consequential fuel sheath strain
- avoidance of consequential fuel oxidation
- avoidance of consequential constrained axial fuel-string expansion exceeding fuel channel service level limits or resulting in fuel sheath to pressure tube contact or significant changes to fuel configuration for removal of residual heat at temperatures below fuel sheath melting
- avoidance of consequential fuel sheath to pressure tube contact
- avoidance of consequential fuel sheath melting or embrittlement failures
- avoidance of consequential fuel central melting
- limit extent of liquefaction
- avoidance of consequential fuel dispersal
- avoidance of superprompt criticality

4.2.17 Associated Regulatory Requirements[44]

In the analysis:

- demonstrate that the analysis requirements[45] of Regulatory Document R–7[46] for the containment system are met
- demonstrate that the analysis requirements[47] of Regulatory Documents R–8[48] and R–10 for the shutdown systems are met[49]
- demonstrate that the analysis requirements[50] of Regulatory Document R–9[51] for the ECCS are met
- demonstrate that, for pressure retaining components, the appropriate service limits of Regulatory Document R–77 and the applicable engineering codes and standards are not exceeded.

4.2.18 Validity of the Analysis

In the analysis:

a) identify key safety analysis assumptions, parameters (including process parameters), models, and methods for which the operating procedures and performance of the mitigating systems are most sensitive, including the degree of sensitivity to each

b) account, to within a high probability, for bias and variance in a)

c) assess the sensitivity in a) (except for Class 5 events) by demonstrating that the requirements of the next higher numbered event class are not exceeded with a very high probability[52]. If the margins by which these requirements are met are relatively small, reach acceptance with the AECB to determine whether further analysis is necessary

d) identify and conservatively account for the bias and variance (including test instrument error, detector and instrument loop error, and simulation error) in the allowances for tolerances[53] on parameters used by mitigating systems, and identify the operating procedures[54] that ensure that the performance of mitigating systems is not impaired

e) identify and account conservatively for the numerical accuracy of the calculational methods

f) identify the simplifications and approximations used in the mathematical models and calculational methods

g) identify the conservatism used in empirical correlations and mathematical models.

4.2.19 Safety Margins

Use demonstrably conservative safety margins and safety factors in accordance with good engineering practice and available codes and standards:

- identify limitations on attainable confidence levels of tolerances on analysis parameters
- identify limitations of analysis idealizations such as unquantified phenomena
- identify how the safety margins account for these limitations.

4.2.20 Mathematical Models and Calculational Methods

Verify that the mathematical models and calculational methods (including input data) represent a conservative[55] prediction for each of the safety analysis requirements, which may be a best estimate with a conservative tolerance for bias. All physical phenomena should be accounted for, and simplifications should be appropriate.

4.2.21 Conservative Assumptions

When choosing conservative assumptions and error tolerances, identify and account for the presence of each effect listed in Table 4.7 separately. (Note that this table is not exhaustive.)

Table 4.7: Effects to Account for When Choosing Conservative Assumptions

Effect	Examples
thresholds	• criticality • yield strengths • dryout • phase transitions • flow regimes • coalescence • quenching • surface tension • cavitation • minimum pump suction head • instability • turbulence • chaos • sonic velocity • choking • set points • instrument detection limits • vessel capacity • contact of components
timing	• coincidence with other events • logic • operator delays
competing effects	• cancel • counterbalance • neutralize • oppose

Table 4.7: Effects to Account for When Choosing Conservative Assumptions (cont.)

different failure mechanisms	• collapse • buckling • non-uniform ballooning • athermal strain • creep • fatigue • stress corrosion cracking • embrittlement • erosion • corrosion • dissolution • melting • volatilization
different reactions	• nuclear • chemical
different transport processes	• inertial • laminar and turbulent convection • diffusion • waves • scrubbing • radiation • thermophoretic • gravity • pressure • capillarity • Brownian motion • speciation

...continued

Table 4.7: Effects to Account for When Choosing Conservative Assumptions (cont.)

different transport processes	• volatization • evaporation • absorbtion • sublimation • aerosol • condensation • deposition • percolation • electrostatic • osmosis • buoyant • suspension • dissolution • chemical reaction
structural integrity	• each barrier that surrounds the fuel

4.2.22 Verification

Identify the type and extent of the verification of the calculational methods.

4.2.23 Validation

Identify the type and extent of the validation of the mathematical models. Regardless of the conservative assumptions on parameters, perform a validation for the various physical phenomena predicted by the safety analysis taking effect over the range of conditions, such as temperatures, pressures, and powers. Validate interactions between the phenomena over the applicable range. Justify the basis for scaling experimental data. (Code-to-code comparisons are useful but do not constitute adequate validation. Base validation on applicable operating experience, commissioning activities, or experimental data and analyses.)

4.2.24 Commissioning Tests

Identify the credited commissioning tests[56] as verification of the results of the analysis. Also identify additional tests that could be performed as a further verification.

4.2.25 Data

Identify the input assumptions and data, and provide a rationale for the selection of input assumptions.

4.2.26 Intermediate Results

Identify the transient values of important variables[57] and the timing of key events[58].

4.2.27 Acceptance Criteria

Demonstrate, within a high probability, that:

- the dose and release limits of Table 4.8 are not exceeded for the period 30 days after the initiating event.
- the associated regulatory requirements[59] in Table 4.9 are met.

Table 4.8: Dose and Release Limits[60]

Requirement	Event Class				
	1	2	3	4	5
effective dose (mSv)	0.5	5	30	100	250
lens of the eye (mSv)	5	50	300	1,000	1,500
skin (mSv, averaged over 1 cm^2)	20	200	1,200	4,000	5,000
30 d emissions of liquid effluent are within the derived annual emission limits for normal operation	•	•	N	N	N

• — the limit shall be met by the worst failure sequence in the event class.

N — not required.

d — day.

Table 4.9: Associated Regulatory Requirements and Derived Acceptance Criteria

Requirement	Event Class				
	1	2	3	4	5
containment below positive design pressure***	•	•	•	•	•
containment above negative design pressure	•	•	•	•	•
avoidance of consequential damage to reactor systems from impairment of containment integrity	•	•	•	•	•
avoidance of consequential damage to containment structure	•	•	•	•	•
avoidance of consequential hydrogen explosion or deflagration	•	•	•	•	•

Table 4.9: Associated Regulatory Requirements and Derived Acceptance Criteria (cont.)

avoidance of consequential loss of ECCS integrity	•	•	•	•	•
avoidance of consequential damage to shutdown systems	•	•	•	•	•
service level limit crediting the first shutdown system that trips*	B	C	C	D	D
service level limit only crediting the second shutdown system that trips*	C	D	D	D	D
service level limit on valves that must change state	B	B	B	B	B
avoidance of consequential loss of primary heat transport system integrity*	•	•	•	•	•
avoidance of consequential loss of integrity of any fuel channel*	•	•	•	•	•
fuel channel configuration for removal of residual heat* †	•	•	•	•	•
avoidance of consequential loss of integrity of any fuel sheath*	•	•	•	•	N
avoidance of further fuel damage after ECCS re-establishes adequate cooling* †	•	•	•	•	•
fuel configuration for removal of residual heat* †	•	•	•	•	•
maintain spent fuel pool cooling (no boiling or uncovery)	•	•	•	•	•
spent fuel maintained subcritical	•	•	•	•	•
reactor maintained subcritical after shutdown	•	•	•	•	•

* For events where the initiating event is in a single fuel channel, its feeder piping, or fuelling machines, these requirements do not apply to that channel or the fuel associated with it.

† For events that include failure of the ECCS, this requirement does not apply.

*** For events where the initiating event is the failure of any pipe in the boiler feedwater or steam systems, and does not release radioactive materials into containment, this requirement does not apply.

• Meet this limit.

• Limit the extent, severity, and duration of exceeding the limit by the mitigating systems.

N Not required.

B
C } Level B, C and D Service Limits are defined in the General Requirements under Section III of the *American Society of Mechanical Engineers Boiler and Pressure Vessel Code* (ASME Code).
D

Notes

1. In the shutdown state, some systems continue to operate while others are out-of-service. Consequently, certain initiating events do not apply to the shutdown state.

2. Turbine overspeed protection is also a mitigating system, but is typically credited with a higher reliability than these systems.

3. For the trip parameters to be diverse, they should not share the same sensor.

4. Overpressure protection is a case in which relaxed requirements are specified for the second shutdown system that trips. Determine the effectiveness of each shutdown system acting alone.

5. For example:

    - Do not credit the reactor regulating system (RRS) to supplement the shutdown system but demonstrate that normal operation of the RRS does not render the shutdown system ineffective.
    - The partial or incomplete operation of one shutdown system (including any pressure relief valves connected to it) should not render the other shutdown system ineffective.

6. For example, analyse failures of the primary coolant inventory control system, and demonstrate that normal operation of the primary coolant inventory control does not render the ECCS ineffective.

7. The combination of a single failure plus a variance allowance at a practical confidence level (e.g., 95 percent) is expected to keep the analysis reliability higher than the system reliability.

8. An example of an analysis for which certain transient plant states have been accepted as random variables (e.g., power ripple from refuelling and detector drift) is the regional or neutron overpower trip for slow failure of reactor power control.

9. Make tolerance for instrument error at a proportion of approximately 95 percent at 95 percent confidence.

10. Make allowances for bias on the calculational method at approximately 95 percent confidence instead of the mean.

11. For example, assuming the minimum amount of water in the dousing tank is not conservative in assessing cross-link effects from flooding.

12. Consider temperatures within their limits in the operating envelope, refuelling ripple, and instrument drift as biases, not random variables (i.e., when the plant is put in a state, the probability of that state is "one" and the classification of the event is determined by the probability of the event.)

    For example, do not place a failure sequence consisting of an initiating event during shutdown operation in a higher event class owing to an anticipated low frequency of occurrence of the shutdown state.

13. For example, a partial failure that maximizes fuel and pressure tube temperatures in the short term when the pressure is high may cause more contact of the pressure tube with the calandria tube. This may cause lower fuel and pressure tube temperatures in the long term when the pressure is low and hence may lower the fission product release if long term cooling is lost.

14. The location and orientation of the break are important for determining the cross-link effects of pipe whip and jet forces.

15. Acceptable interpretations are any large proportion (e.g., 90 percent of the time or 95th percentile at 95 percent confidence).

16. Certain low probability failure modes such as open airlock doors and loss of vacuum are analysed, but a dose or release limit are not assigned to failure sequences that include them.

17. Safety analysis requirements for extremely low probability accidents are outside the scope of this document.

18. AECB, *Overpressure Protection Requirements for Primary Heat Transport Systems in CANDU Power Reactors Fitted with Two Shutdown Systems*, Regulatory Document R-77.

19. If servicing is required to fulfil the credited mission time, include an assessment to show that safety-related systems can be serviced to prevent loss of function in the long term; otherwise analyse eventual failure of the system.

20. "Designed to meet the intended function" includes consideration of the effects of ageing.

21. "Qualified to withstand all cross-link effects" includes environmental qualification, seismic qualification, and qualification against the dynamic effects resulting from pipe breaks.

22. For example, ECCS actuation on low pressure may be impaired for a small loss of primary coolant if pressure control is not qualified and fails high, resulting in pressure failing to drop to the low-pressure set point.

23. "Minimum allowable performance standards" means the set of operating limits or the range of conditions established for components or subsystems that define the minimum acceptable states for credited components or subsystems.

24. Extend dose calculations, however, beyond 30 days to include the committed dose from radiological releases that occurred during the first 30 days.

25. This includes reactor power and isotopic composition of the fuel, coolant, moderator, reactivity devices, and detectors.

26. Examples of assumptions are: shutoff rod drop characteristics, poison curtain growth, instrument delays, detector response characteristics.

27. Include the effects of all displacements of fuel, coolant, moderator, and reactivity devices; changes in temperature and density; and nuclear reactions.

28. Although the dominant heat source in the plant is nuclear, the normal stored heat as well as electrical and chemical energy can be significant.

29. Take into account possible changes of heat sink during the event.

30. The loads may be nuclear, chemical, thermal, mechanical, electrical, and gravitational.

31. Nuclear, thermal-mechanical, and chemical effects can alter material, thermal, elastic, tensile, and fracture properties of each weld, heat-affected zone, and shell.

32. This includes the physical form or phase of each group of radioactive materials.

33. Take into account chemical reactions and phase transitions.

34. Include the number and timing of fuel failures in release.

35. Do not exceed 10^2 TBq of ^{137}Cs release. (Finnish Centre for Radiation and Nuclear Safety, Decision of the Council of State on the general regulations for the safety of nuclear power plants (395/91), 1991 February 14; UK Nuclear Installations Inspectorate, Safety Assessment Principles for Nuclear Plants, 1992).

36. The calculation should account for any necessary post-accident response activities. Do not exceed the annual dose limits for occupational exposures as set out in regulation. Base

internal dose conversion factors on ICRP 68.

37. The release duration is 30 days or less.

38. A method for the dose calculation is described in Radiation Protection Bureau, Health Canada, 1998, *Recommendations on Dose Coefficients for Assessing Doses from Accidental Radionuclides Releases to the Environment*, ICRP 72 and CAN/CSA–N288.2–M91. Also include dose from re-suspension of deposited radionuclides.

39. A method for the dose calculation is described in ICRP 72 and CAN/CSA–N288.1–M87. Also include dose from re-suspension of deposited radionuclides.

40. The annual dose may indicate the long-term offsite intervention required for a failure sequence, but no safety analysis limit applies to this calculation.

41. The collective dose may indicate the extent of the offsite intervention required for a failure sequence, but no safety analysis limit applies to this calculation.

42. To demonstrate compliance with the dose and release limits of Table 1.8, it may be necessary to define more conservative limits such as a maximum fuel sheath temperature.

43. The confidence and prediction intervals are wider at the edge of the range of experimental support or applicability.

44. Table 4.9 contains a summary of the associated regulatory requirements, generalized to the five event classes.

45. The analysis requirements for the containment include: structural integrity, environmental conditions, availability, hydrogen concentration, separation and independence, shielding, instrumentation, maintenance, and operating procedural requirements.

46. AECB, *Requirements for Containment Systems for CANDU Nuclear Power Plants*, Regulatory Document R-7.

47. The analysis requirements for the shutdown systems include:

- primary heat transport system integrity
- fuel integrity
- environmental conditions
- availability, separation and independence

- instrumentation
- maintenance and operating procedural requirements.

For example: a loss of primary heat transport system integrity shall not result from over-pressure or any fuel failure mechanism, such as excessive fuel temperatures or fuel breakup; each shutdown system shall ensure that fuel in the reactor does not fail as a consequence of failure of reactor control systems.

48. AECB, *Requirements for Shutdown Systems for CANDU Nuclear Power Plants*, Regulatory Document R-8.

49. Of particular importance is the demonstration of at least two effective and diverse trip parameters on each shutdown system for all plant states of normal operation.

50. The analysis requirements for ECCS include:

- fuel channel integrity
- fuel integrity, fuel and fuel channel configuration
- prevention of further damage to fuel
- environmental conditions
- availability
- separation and independence
- inadvertent operation
- shielding
- instrumentation
- maintenance and operating procedural requirements.

For example, the ECCS shall be capable of maintaining fuel channel integrity following failure of any pipe or header in the primary heat transport system. There shall be no fuel failure in the reactor owing to a lack of adequate cooling following the failure of any feeder pipe in the primary heat transport system (except in the channel associated with the feeder failure).

51. AECB, *Requirements for Emergency Core Cooling Systems for CANDU Nuclear Power Plants*, Regulatory Document R-9.

52. Examples of sensitivity assessments are:

- Worst or conservative weather — a weather scenario that emits a dose (time integrated concentration) that is exceeded, at most, 10 percent of the time. Re-analyse the same failure sequence using a weather scenario that emits a dose that is exceeded, at most, 1 percent of the time, and do not exceed the dose limits of the next higher numbered event class.
- Probability of a fuel element failure — if the probability of a fuel element failure, summed over the core, from an event Class 2 is less than 10 percent and there is a less than 1 percent probability that the number of fuel element failures is greater than 50,000, then no fuel failures is an acceptable conservative assumption. Re-analyse the failure sequence assuming that there are 50,000 fuel element failures, and do not exceed the dose limits of event Class 3;
- 90 percent probability of avoidance of fuel sheath dryout — acceptable for the first high quality trip parameter of Class 2 events but attain 99 percent for Class 1 events; and
- Variance on the worst plant state — account for this variance at 90 percent probability. This includes mathematical model and calculational method biases, and variance in the boundary of the operating envelope. Variance on the boundary includes instrumentation variance, calibration variance, and the probability of failure of safety-related systems (e.g., such as operating procedures), that ensure the plant state remains within its operating envelope. Re-analyse the future sequence conservatively with such variance taken into account at 99 percent probability, and do not exceed the dose limits of the next higher numbered event class.

53. "Parameter tolerance" is the magnitude of the difference between the nominal set point or nominal parameter value (process parameter), and the value at which the system is considered to be impaired. (The impairment value should have as large a safety margin to the safety limit as practicable.)

54. For plants under design for which no operating procedures exist, specify operating procedures for credited operator actions.

55. Assumptions that result in a conservative prediction for one analysis may result in non-conservative results for another. For example, use of a break discharge model that predicts more energy and mass discharge than would actually occur may be conservative for fuel sheath strain and containment integrity but not for blinding of containment isolation

detection or challenge to fuel channel integrity. Similarly, a lower bounded critical heat flux correlation may be conservative for fuel and channel temperatures but not for transient boiling phenomena such as over pressure and void reactivity.

56. Use commissioning tests to verify the results of the analysis to the extent that is practicable without compromising reactor safety.

57. Important variables may include:

- reactivity
- pressures, temperatures, and inventories within the fuel, the various pressure retaining components, and containment
- coolant flow rates and pump behaviour
- release and distribution of radioactive material.

58. Key events may include:

- reactor trip
- ECCS initiation
- containment isolation
- pump trip
- operator action
- fuel dryout
- fuel failure
- pressure tube ballooning.

59. The majority of the associated regulatory requirements are in Regulatory Documents R–7, R–8, R–9 and R–77.

60. Only individual dose and release limits related to individual sequences are specified in this guide. Collective dose limits are not specified because the individual dose limits:

- apportion the effective dose to a hypothetical, most-exposed member of the critical group of the public from events of concern (other than failure of certain passive components and event combinations) to a fraction of the annual dose limit, assuming the recurrence period of such events is maintained more than a year, by corrective action if necessary
- limit the lifetime dose to any member of the public from an event of concern

involving failure of certain passive components or involving event combinations (including failure of a special safety system) to be an acceptable increment in lifetime dose

- avert any deterministic effect, thereby avoiding its collective detriment and the difficult and controversial specification of a collective detriment from more severe exposures.

5. Probabilistic Safety Assessment

This section provides general information about how a Probabilistic Safety Assessment (PSA) is to be used in a safety analysis.

5.1 Scope

Submit a full-scope level two Probabilistic Safety Assessment[1] (i.e., assessment of core damage and containment damage from all plant states) to the AECB after the design and operating procedures have been finalized. During the operational phase, keep the PSA up-to-date. Submit the updates in accordance with a schedule acceptable to the AECB.

Conduct and document the PSA according to internationally-recognized best practices.

5.2 Use of the PSA in Analysis

In concert with the safety analysis, the analyst reviews the PSA to:

- confirm that the list of failure sequences identified by the systematic review was complete for event classes 1 through 5
- assist in confirming that the classification of events and the associated reliability assumptions were conservative
- identify the failure sequences that dominate the cumulative frequency of serious process failures
- demonstrate that the cumulative frequency of serious process failures is less than the required target[2]
- identify the failure sequences in which the moderator is used as a heat sink by multiple fuel channels to maintain their integrity
- calculate the total demand frequency[3] of the moderator as a heat sink by multiple fuel channels to maintain their integrity
- identify relative plant weaknesses
- identify failures that dominate the unreliability of each safety-related system
- calculate the reliability[4] of each mitigating system[5]

- identify the conservative assumptions and simplifications that are used in the PSA, and estimate their effects on the results[6]
- identify any safety-related items whose importance is not apparent because of such assumptions.

Notes

1. In a PSA, component failure and external event data are collected and a plant logic diagram and system fault trees are analysed to determine the probabilities of:

   - exceeding various plant damage states
   - release levels (such as those that correspond to doses to an individual, contamination, or harm to the environment)
   - collective detriment levels (when the doses to an individual result in deterministic effects).

   The PSA should include the switch yard as well as the plant because of dependencies.

2. Specification of the target is outside the scope of this document. A frequency of one in every three years is set out in D. G. Hurst and F. C. Boyd, *Reactor Licensing and Safety Requirements*, AECB–1059, June 1972.

3. The total demand on the moderator system by multiple channels should be less than 10^{-4} per year.

4. Before the design and operating procedures have been finalized, the designer may use a preliminary PSA to set reliability requirements and operational limits.

5. Of particular importance are the availability and reliability of the special safety systems (including their support systems) and heat sinks. Other important factors include the probability of the failure of pressure tube(s) to suffer from hydride cracking, and the consequential probabilities of the failure of boiler tube(s), fuel dryout during overpower, failure of fuel channel(s), and failure of containment.

6. The PSA data and assumptions should be a best-estimate rather than conservative.

Glossary

The following definitions constitute a partial list of terms used in this document. Additional definitions can be found in Regulatory Documents R-7, R-8 and R-9.

Actuation Parameter — the parameter level that triggers the activation of a mitigating system (also referred to as "set point").

Best Estimate — unbiased estimate of mathematical model and calculational method. (Estimation réaliste)

Common Cause — a condition in which multiple effects on systems, components, structures, or procedures result from a single cause. (Cause commune)

Conservative Estimate — a mathematical model or calculational method that is biased to yield more severe consequences for a particular requirement. (Estimation conservatrice)

Crediting — to acknowledge that something (e.g., a mitigating system) is responsible for causing an action (e.g., mitigating an event). (Créditer ou considérer)

Cross-link Effect — the causal effect of the operation or failure of a system, component, structure, or procedure on other systems, components, structures, or procedures. A cross-link effect can be created by an initiating event, an event combination, a common cause, or the unexpected consequence of normal operation. (Effets de mode commun)

Dependency — a thing that is correlated with or is conditional on another. (Dépendance)

Event of Concern — a credible event that, in the absence of all mitigating provisions, would lead to systematic fuel failures or a significant release of radioactive materials from the nuclear power plant. Systematic fuel failure means that fuel with no prior defects fails as a result of the event. A significant release is equal to the derived release limits. (Événement grave)

Failure — a change in the characteristics of a system, component, structure, or procedure such that it becomes unable to carry out its minimum intended function or performs an undesirable function. This includes partial and total change of function, which could be latent, coincidental, prolonged for 30 days, delayed, temporary or intermittent. Latent failures include prior failures such as errors in control logic, testing, operating, maintenance and failure to restart. Coincidental failures include failures such as operator inaction. Mission failures are treated explicitly as combinations of events occurring within 30 days. (Défaillance)

Loss of Reactor Primary Coolant (Perte de fluide caloporteur primaire du réacteur)

Very Small Loss of Reactor Primary Coolant — a discharge rate up to and including the makeup capability of one primary feedwater pump. (Très petite perte de fluide caloporteur primaire)

Small Loss of Reactor Primary Coolant — a discharge rate beyond that of a very small loss of primary coolant up to and including that which would result from a double-ended guillotine break of the largest fuel channel feeder. (Petite perte de fluide caloporteur primaire)

Large Loss of Reactor Primary Coolant — a discharge rate beyond that of a small loss of primary coolant up to and including that which would result from a double-ended guillotine break or a longitudinal break of the largest pipe or header. (Grosse perte de fluide caloporteur primaire)

Mitigating Provisions — a subset of safety-related items associated with the detection or mitigation of failure sequences. Includes special safety systems, standby emergency systems, mitigating process systems, process systems that do not change state to mitigate the consequences of an event, and certain passive components, structures, and procedures. (Système d'atténuation)

Mitigating Process System — a process system that must respond by changing state, increasing its capacity, or increasing its speed to mitigate the consequences of an event. (Système de procédé d'atténuation)

Standby Emergency System — a routinely tested standby emergency system other than the special safety systems. (Système d'urgence en attente)

Negative Reactivity Insertion — a reduction of reactivity. (Insertion de réactivité négative)

Normal Operation — all planned states that the nuclear power plant may be in as a result of normal operating procedures approved by the licensee. Includes all shutdown, power operation (start-up, power manoeuvring, steady state, shim, and load following), initial, intermediate, and end-of-life states during which refuelling, calibration, testing, maintenance, and inspection may also be occurring. (Exploitation normale)

Operating Procedures — written procedures and data that define the methods, means, and operating limits of systems, components, and structures for normal operation (normal operating procedures including testing and maintenance procedures) and during anticipated operating occurrences or events of concern (emergency operating procedures). (Procédures d'exploitation)

Plant State — configuration of components of a power plant. (État de centrale)

Qualified Component — a component that is able to withstand the effects of an event to the extent that it meets the safety criteria. (*Composant qualifié*)

Safe Shutdown State — the long-term stabilized condition in which:

a) the fuel is maintained conservatively subcritical.

b) the nuclear power plant is cooled [illegible]

c) the heat generated in the nuclear power plant is being removed to an effective, long-term heat sink such that the thermal design limits, design conditions, and regulatory requirements of the mitigating systems being credited are not exceeded.

d) the release rate of radioactive materials from the nuclear power plant site is controlled, the annual emission of liquid effluent is less than one tenth of the derived annual release limits for normal operation, and the weekly dose to a hypothetical most-exposed member of the critical group at or beyond the site boundary will remain less than two microsieverts (μSv).

e) the operator is able to monitor the nuclear power plant and act in accordance with operating procedures. (*État d'arrêt sécuritaire*)

Safety-related Item — a system, component, structure, or procedure (operator actions) and its support systems (including the special safety systems and their support systems) associated with initiation, detection, or mitigation of any failure sequence that will precipitate an event of concern. Examples of support systems are: instrument air, electrical power, cooling water, fuel, lubricants, chemicals, test and calibration instruments. (*Système relié à la sûreté*)

Serious Process Failure — a failure of a safety-related system that, in the absence of all special safety systems, would lead to systematic fuel failures or a significant release of radioactive materials from the nuclear power plant. Systematic fuel failure means that fuel with no prior defects fails as a consequence of the event. A significant release is equal to the derived release limits. (*Défaillance grave de système de procédé*)

Set Point — *See Actuation Parameter*. (*Seuil*)

Special Safety System — one of the following systems: shutdown system, emergency core cooling system (ECCS), and containment system. (*Système spécial de sûreté*)

Worst Plant State — the plant state that yields the most severe consequences for a particular requirement. (*Pire état de centrale*)

Appendix A: Probabilistic Technique for Classification of Events

Address the guidelines described in this Appendix if the probabilistic technique for event classification is chosen as an alternative[1] to the classification scheme described in this guide. Do not confuse these guidelines with the PSA described in Section 5.

A.1 Failure Data

Determine failure data by completing the following tasks:

- Identify the probability of failure and dependency data for safety-related items and their 95 percent upper confidence limits.
- Identify failure modes, number of failures, in-service times, down times and repair times.
- Identify credits for maintenance activities, surveillance activities (panel checks, routines, tests, inspections), item condition, item duty, item configuration and repair times.
- Derive statistical data on the failure of items from a relevant population.
- Identify and justifying the population.
- Justify the use of any model, such as the exponential model or Weibull model.

A.2 Ageing

Use failure probabilities that correspond to the worst tolerable condition of components during the life of the plant. Do not average failure probabilities over the life of the plant or across plants that performed in the worst condition tolerable and plants that performed better. Use plant-specific data only for plants that are in the operation phase and that have accepted inspection strategies and fitness for service criteria.

A.3 Plant State Data

Determine plant state data by completing the following tasks:

- Identify the plant state data.
- Record data over a sufficiently long period of time in order to include events occurring over the life of the plant at the required probability.

The probabilities of plant states are taken at the upper 95 percent confidence limit.

A.4 Surveillance, Inspection and Testing

Verify failure, plant state probabilities, and their confidence intervals through an in-service surveillance, inspection, and testing program, to the satisfaction of the AECB.

A.5 Event Class Probability Ranges

The probability range for each event class is given in Table A.1.

A.6 Event Probability

Classify each initiating event and combination of events, occurring within 30 days of each other, according to their mean annual probability at the upper 95 percent confidence limit.

The annual probability is the sum of all failures resulting in the same loss of, or undesirable, system functional capability as opposed to the subdivision of events by plant response[2]. This probability may also include the probability of the plant state and the probability of the mitigating system capability, but not the probability of the weather scenario.

A.7 Event Subdivision

An event may be subdivided in order to classify a specific failure with a different plant response in a higher numbered event class (to a maximum of Class 5) if the failure has a low probability, relative to other events having the same loss of, or undesirable, functions, and the failure is specifically addressed by design, fabrication, installation, operation, testing and maintenance to the satisfaction of the AECB.

A.8 Common Cause Event Probability

Define common cause events (single or combination common cause events occurring within 30 days of each other) appropriate to each of the event classes. Classify each event and combination of events according to their mean annual probability at the upper 95 percent confidence limit. The annual probability may also include the probability of the plant state and the probability of the mitigating system capability, but not the probability of the weather scenario[2].

A.9 Mitigating System Capability

For each event, define event combinations with degraded mitigating system performance during a 30 day period that are appropriate to each of the higher numbered event classes. The appropriate maximum functional capability of the mitigating systems corresponds to the lowest probability of the range (shown in Table A.1) for the event class in which the combination is being analysed. Use the mean annual probability of the event combination at the upper 95 percent confidence limit.

Credit each mitigating system or component of that system using:

- its operational reliability if the system or component continues to operate under conditions similar to those that existed prior to the initiating event; and
- availability and reliability targets, which are to be verified by in-service testing if the system or component is required to start operating, change state, or change its range or speed of response in order to mitigate the consequences of the failure sequence.

A.10 Plant State

For each event, define combinations that are appropriate to each of the higher numbered event classes corresponding to plant states with more severe consequences. Include allowable plant states and beyond allowable plant states that have occurred or are anticipated to occur. The appropriate combination of the event and the plant state corresponds to the lowest probability of the range for the event class (shown in Table A.1) in which the combination is being analysed. Use the mean annual probability of the combination at the upper 95 percent confidence limit.

Do not credit the probability of allowable plant states unless the following minimum requirements are met acceptably to the AECB:

- the plant variable is monitored;
- the plant variable is controlled to a single mean and standard deviation; and
- the operating procedures identify the controlled variables, their range and duration limits, and alarm levels or test intervals.

A.11 Transient Plant States

Classify combinations of events with a transient plant state that results from deliberate operator action to change the mean of a plant variable and plant states that are necessarily entered (such as starting up, fuelling, and shutting down) by their probability only if dependency data are available and accounted. Credit for the

probability of plant states having different variable means if the frequency and duration of the mean is limited[4] by the operating procedures. If the mean probability at the upper 95 percent confidence limit of such a combination is less than the lower limit of event Class 5, analyse the combination or show that it is to be bounded by a more limiting event (no dose limit applies).

A.12 Instrument Tolerance

Include allowances for instrument tolerances in plant states. These are normally evaluated at a proportion of 95 percent with a confidence limit of 95 percent. It may be impossible to define combinations of events with higher proportions of instrument tolerance for higher numbered event classes. In such cases, propose surrogate combinations for each of the higher numbered event classes. Surrogates to be used for instrument tolerance at a higher confidence limit include a second diverse mitigating system actuation parameter, degradation of mitigating system functional capability, and miscalibration of instruments.

A.13 Range of Plant States

A range of plant states may be defined for which no credit is taken for their probability. However, if the consequences are more extreme outside this region, account for a tolerance on the boundary of this range.

A.14 Weather Scenarios

For each event, define combinations of events and 30-day weather scenarios with probabilities that are appropriate to each of the higher numbered event classes. The probability of the combination of the event and weather scenario is one tenth of the lowest probability of the range (shown in Table A.1) for the event class in which the combination is being analysed. Use the mean annual probability of the event combination at the upper 95 percent confidence limit.

A.15 Dependencies

Identify and account for dependencies between the plant state, instrument error, calculational methods, weather scenarios, initiating events, event combinations, event sequences, and failures of safety-related systems, including operator errors. Use the dependency at the upper 95 percent confidence limit.

A.16 Cross-link Effects

For each event having cross-link effects that are a function of probability, define event combinations appropriate to each of the higher numbered event classes that have increased cross-link effects on mitigating system performance. The appropriate maximum functional capability of the mitigating systems corresponds to the lowest probability of the range (shown in Table A.1) for the event class in which the combination is being analysed. Use the mean annual probability of the event combination at the upper 95 percent confidence limit.

A.17 Common Cause Failure Limitation

Place a common cause failure limitation on the claimed failure probability of systems that use redundant, identical components or procedures. Reflect the complexity, novelty, diversity, separation, independence, and testing of the systems.

A.18 Calculational Methods

Allow for bias in calculational methods at high confidence limits (95 percent). In higher event classes, assess sensitivity analysis, degraded mitigating system functional capability, a second diverse mitigating system actuation parameter, and worse plant states as surrogates for calculational tolerances of higher confidence.

A.19 Standards

Use internationally recognized standards, as accepted by the AECB. Meet the following rules:

- models for human action reliability reflect the complexity of the task and relevant factors, such as environmental conditions and level of stress
- assess the effects of uncertainties in the data and assumptions in modelling the overall result
- assess the effect of combinations of factors as a function of probability
- the nuclear power plant reference design and operating procedures (configuration) are consistent with the design and procedures used in the deterministic analysis.

Table A.1: Event Class Probability Ranges

Event Class	Annual Event Probability
1	more than 10^{-2}
2	10^{-2} to 10^{-3}
3	10^{-3} to 10^{-4}
4	10^{-4} to 10^{-5}
5	10^{-5} to 10^{-7}

Notes

1. Owing to the increased effort required to conduct a probabilistic event classification by the analyst, operator, and regulator, probabilistic event classification should only be done on a case-by-case basis using the guidelines in this appendix. A combination of the classification described in the guide and the guidance described in this appendix can also be used as an alternative.

2. The various failures that have the same loss of system functional capability may have substantially different plant responses.

3. If the common cause event is a weather scenario, credit the probability of the weather scenario in as much as it determines the weather scenario for 30 days after the common cause event.

4. The probability of certain shutdown states, for example, may not be credited because their duration may be indefinite.

   The probability of power peaking during power manoeuvring may be credited, but the probability of power manoeuvring may not be.

5. If data for the dependency does not exist, the probability of the dependency is "one".

Appendix B: Limiting Events

The tables contained in this Appendix describe how limiting events for plant parameters and operating procedures are identified.

Table B.1 outlines the information to be reported for each functional requirement of each event, to demonstrate which events are limiting for a given parameter in the design or operation of the reactor.

Using Table B.1 for reference, identify the functional requirements of the mitigating systems that deal with each event, including:

- whether the source of the functional requirement is a regulatory requirement, design decision, established practice, assumption in the safety analysis, or the edge of the range of analysis support.
- whether the method used to show that the functional requirement is met is through an analysis, an assessment relative to events that are more limiting, an experiment, or an operational experience.
- the method used to account for error.
- the limited design and/or operating procedure parameters for the event.
- the limits on the operating parameters.
- the margin, relative to the functional requirement, that accounts for the effect of variances and tolerances.

Table B.2 shows a default[1], partial[2] list of events in the five event classes. Table B.3 shows common cause events. The tables also show the functional requirement or limiting effect that is used to set each limited parameter. (They neither show key modelling parameters or the conservative direction for their tolerances nor plant states such as shim.)

Table B.1: Layout of Support for Each Limiting Event

Functional Requirements	Source (as applicable)	Method (as applicable)	Parameters (as applicable)	Limits	Margin
Functional requirements of each mitigating system	• regulatory requirement • design decision • established practice • safety analysis assumption • range of analysis support	• analysis including error analysis • assessment • experiment • operational • experience	• design • operational	value	value

Table B.2: Partial List of Limiting Events in Class 1

System/Component Failure of:	Limited Plant Parameters	Functional Requirements or Limiting Effects
dual computer control	fail-safe computer output positions	safe shutdown state
	operating procedures	
reactor power control	maximum power boost	fuel failure
	shutdown system maximum ion chamber set point	coolant boiling
boiler pressure control	shutdown procedure	heat sink
boiler inventory control	procedure to prevent water carry-over	water carry-over
de-aerator inventory control	operator action	heat sink
primary coolant pressure control	primary coolant high-pressure trip setpoint	primary coolant pressure
	shutdown procedure	heat sink
	containment isolation procedure	dose
	primary coolant pump trip maximum delay	primary piping fatigue
	minimum pressure setpoint	
	minimum primary coolant bleed condenser relief valve capacity	bleed condenser pressure
	minimum pressurizer relief valve capacity	pressurizer pressure
primary coolant inventory control	containment isolation procedure	dose
	minimum primary coolant relief valve capacity	primary coolant pressure
residual heat removal system temperature control	time for alternative heat sink procedure	sheath temperature

...continued

Table B.2: Partial List of Limiting Events in Class 1 (cont.)

System/Component Failure of:	Limited Plant Parameters	Functional Requirements or Limiting Effects
moderator temperature control	moderator high level trip setpoint	dose
	containment isolation procedure	
	calandria strength	shutdown system integrity
	operating procedures	D_2O freezing
compressed air (instrument or service)	emergency compressed air	heat sink
	procedures to control liquid flow, moderator flow, and primary coolant feed	D_2O freezing, heat sink
	minimum primary coolant relief valve capacity	primary coolant pressure
	minimum primary coolant bleed condenser relief valve capacity	bleed condenser pressure
service water flow	emergency service water	heat sink
	maximum moderator or primary coolant return	dose
	minimum primary coolant relief valve capacity	primary coolant pressure
	minimum primary coolant bleed condenser relief valve capacity	bleed condenser pressure
	shield relief valve capacity	shield pressure
	containment system cooling minimum capacity	containment temperature
trip or valves, causing a loss of service water	shutdown system trips on moderator high temperature	moderator pressure
normal electrical power	standby generator(s) in time and capacity	boiler level

Table B.2: Partial List of Limiting Events in Class 1 (cont.)

System/Component Failure of:	Limited Plant Parameters	Functional Requirements or Limiting Effects
normal electrical power	minimum equipment supplied by Class III emergency electrical power	boiler level
	minimum primary coolant relief valve capacity	primary coolant pressure
	extent of pressure tube flaws	pressure tube integrity
	minimum primary coolant bleed condenser relief valve capacity	bleed condenser pressure
heating, ventilation, or air conditioning	emergency heating, ventilation, or air conditioning	dose, habitability, and qualification
pressure relief valve in a vacuum containment system	containment negative design pressure	containment integrity
	shutdown procedure	ECCS actuation pressure
turbine generator load rejection/control	(bounded by failure of condenser vacuum) maximum primary coolant tritium and iodine	dose
condenser vacuum	time for shutdown procedure	heat sink
	capacity and pressure of safety relief valves	secondary coolant pressure
normal boiler feedwater flow	shutdown system trip setpoint on boiler feed line low pressure and boiler low level	boiler level and reactor primary coolant pressure
	shutdown procedure	

...continued

Table B.2: Partial List of Limiting Events in Class 1 (cont.)

System/Component Failure of:	Limited Plant Parameters	Functional Requirements or Limiting Effects
normal boiler feedwater flow	boiler emergency cooling system water and capacité d'air at minimum pressure, auxiliary boiler feedwater system minimum capacity and maximum boiler connections	boiler level
	emergency service water redundant pump auto start and minimum pressure	boiler level, containment system temperature, moderator system pressure, and shield cooling system pressure, and air conditioning
steam line isolation valve	shutdown procedure	heat sink
	boiler relief capacity	boiler pressure
piping, causing a very small loss of reactor primary coolant	procedures for recovery of primary coolant and containment isolation	dose
	maximum primary coolant tritium and iodine	
seals or valve, causing a loss of reactor primary coolant	(same as loss of reactor primary coolant) isolation of blend condenser	
seals or valve, causing a loss of reactor secondary coolant	extent of boiler tube degradation resulting in boiler tube consequential leak	
boiler tube	(same as very small loss of reactor primary coolant)	dose
	maximum activity in the reactor primary coolant	
	procedures to isolate boiler blowoff and deaerator vents, and depressurize and drain the reactor primary coolant	

Table B.2: Partial List of Limiting Events in Class 1 (cont.)

System/Component Failure of:	Limited Plant Parameters	Functional Requirements or Limiting Effects
pressure tube of any fuel channel assembly	(same as loss of reactor primary coolant)	does
	containment isolation procedure	
primary pressure relief valve(s)	shutdown and depressurization procedures	overpressure
primary system loop interconnect valve or pressurizer connection valve	shutdown procedure	primary coolant level
residual heat removal system (excluding piping failure other than a heat exchanger tube)	alternative heat sink procedure	heat sink
moderator system (excluding piping failure other than a heat exchanger tube)	shield coolant minimum inlet temperature	shield/calandria stress
	shutdown system trip setpoint on moderator high level	moderator pressure
valve or valves causing a loss of moderator water	shut down and isolation procedure	does
reactor shield cooling system (excluding piping failure other than a heat exchanger tube)	shut down procedure	primary coolant system and shutdown system negative
D$_2$O management	maximum tritium concentration	does
	D$_2$O management cost epacts	environmental qualification
	shut down procedure	heat sink
failing readout or ground for fuel channel closure plug	heads power	does

...continued

Table B.2: Partial List of Limiting Events in Class 1 (cont.)

System/Component Failure of:	Limited Plant Parameters	Functional Requirements or Limiting Effects
cooling system of a fuelling machine	containment system isolation valve closure time	dose
	containment system isolation and filtered venting procedure	
	bundle power	
improper transfer of fuel from the reactor core to the irradiated fuel bay, resulting in fuel damage	procedure	

Table B.2: Partial List of Limiting Events in Class 2

System/Component Failure of:	Limited Plant Parameters	Functional Requirements or Limiting Effects
piping, causing a loss of service water	flood protection	heat sink and monitoring
piping, causing a loss of reactor secondary coolant	shutdown system trip setpoint on boiler low level	boiler level and reactor primary coolant pressure
	containment peak pressure	damage to reactor systems
	primary coolant pump trip maximum delay and minimum pressure setpoint	primary piping fatigue
	residual heat removal system capacity	primary coolant temperature
	instrumented secondary coolant relief valve capacity	boiler pressure and primary coolant temperature
	minimum boiler emergency cooling system pressure	
	maximum residual heat removal system temperature	
	boiler emergency cooling system and auxiliary boiler feedwater system minimum connections	boiler level
	auxiliary boiler feedwater system minimum setpoint on boiler low level and minimum capacity	
	turbine building steam venting system capacity, opening time, temperature setpoint, and detector configuration	environmental qualification

...continued

Table B.2: Partial List of Limiting Events in Class 2 (cont.)

System/Component Failure of:	Limited Plant Parameters	Functional Requirements or Limiting Effects
piping, causing a small loss of reactor primary coolant	ECCS high-pressure pump/accumulator and injection minimum setpoint on primary coolant low pressure	containment system instrumented pressure relief valve minimum setpoint on containment high pressure
	ECCS high-pressure pump/accumulator and injection minimum setpoint on low flow	
	ECCS high-pressure pump/accumulator and injection minimum setpoint on pressurizer low level	
	ECCS maximum setpoint on sustained low flow time	
	ECCS maximum setpoint on containment high pressure	
	ECCS boiler cooldown minimum setpoint on primary coolant low pressure	maximum boiler pressure
	ECCS low pressure pump minimum setpoint on primary coolant low pressure	ECCS low-pressure pump run-up before high-pressure pump and injection setpoint
	ECCS low pressure pump maximum run-up time	
	ECCS storage tank minimum level	ECCS net positive suction head of low-pressure pumps in recovery sump
	ECCS storage tank maximum level	flooding
	ECCS heat exchanger maximum actuation time	sump water temperature

Table B.2: Partial List of Limiting Events in Class 2 (cont.)

System/Component Failure of:	Limited Plant Parameters	Functional Requirements or Limiting Effects
inlet piping, causing single channel flow stagnation	minimum ECCS heat sink	reactor power
	maximum channel power	dose, fuel temperature, and pressure tube temperature
	extent of boiler tube degradation resulting in consequential rupture	
	containment system instrumented pressure relief valves maximum setpoint on high containment pressure	
	containment system minimum pressure	
	containment system isolation valve maximum setpoint on high containment pressure	
	containment system isolation valve maximum setpoint on high activity	
	containment system cooling maximum capacity	
	containment system maximum leakage	
end fitting of any fuel channel assembly	containment isolation procedure	dose
residual heat removal system isolation valves	(may bound failure of normal electrical power)	fuel temperature
boiler primary head divider	(may bound failure of normal electrical power)	
ECCS isolation valves	(may bound failure of normal electrical power)	
piping or calandria tube, causing a loss of moderator	moderator maximum tritium concentration	dose
	shield coolant minimum inlet temperature	calandria tube stress
piping, causing a loss of reactor shield coolant	shut down procedure	integrity of primary coolant and shut down systems

Table B.2: Partial List of Limiting Events in Class 3

System/Component Failure of:	Limited Plant Parameters	Functional Requirements or Limiting Effects
piping, causing a large loss of reactor primary coolant	minimum number of fuel bundles in a channel	fuel channel/machine integrity and fuel temperature
	containment instrumented pressure relief valve minimum capacity	dose
	ECCS heat exchanger setpoint on high sump level	dose/backflow to storage tank
large number of boiler tubes	isolation procedure and control of secondary coolant pressure with steam discharge to the condenser	dose
service water flow + emergency service water system	shield coolant maximum inlet temperature	shield coolant water temperature and pressure
	instrumented secondary coolant relief valve capacity	shield pressure and fuel channel integrity
components, causing backflow to ECCS	ECCS design pressure	dose

Table B.2: Partial List of Limiting Events in Class 4

System/Component Failure of:	Limited Plant Parameters	Functional Requirements or Limiting Effects
piping, causing a large loss of reactor primary coolant + Class IV power	reactor power	dose
	minimum moderator flow on loss of Class IV power	calandria tube strain
piping, causing loss of secondary coolant + emergency service water system	service water system capacity	environmental qualification of systems and residual heat removal system heat sink

Table B.2: Partial List of Limiting Events in Class 5

System/Component Failure of:	Limited Plant Parameters	Functional Requirements or Limiting Effects
reactor power control + shutdown system + single failure in the other shutdown system	shutdown system neutron high-log rate setpoint	fuel central temperature
	bundle power	
	secondary coolant relief valve capacity	boiler pressure
	reactor coolant maximum inlet temperature	fuel sheath temperature
	shutdown system overpower detectors	
normal electrical power + shutdown system + single failure in the other shutdown system	shutdown system primary coolant low flow setpoint	fuel sheath temperature
	maximum channel power	
	reactor primary coolant minimum pressure	fuel sheath temperature and shutdown system dual parameter trip coverage
	reactor primary coolant minimum inlet temperature	
	minimum instrumented channel power	
	primary coolant high pressure setpoint	
	minimum channel bearing length	pressure tube axial strain, contraction and rolled joint pullout
pressure tube of any fuel channel assembly + shutdown system + single failure in the other shutdown system	ECCS setpoint on moderator head tank high level	fuel sheath temperature

+ means accompanied by

...continued

Table B.2: Partial List of Limiting Events in Class 5 (cont.)

System/Component Failure of:	Limited Plant Parameters	Functional Requirements or Limiting Effects
piping, causing a loss of reactor secondary coolant + shutdown system + single failure in the other shutdown system	residual heat removal system minimum flow connections	fuel and pressure tube temperature
piping, causing a small loss of reactor primary coolant + shutdown system + single failure in the other shutdown system	shutdown system trip setpoint on primary coolant low pressure	fuel sheath temperature
	shutdown system trip setpoint on flow-reduced neutron overpower	
	shutdown system trip setpoint on pressurizer low level	
	reactor primary coolant maximum pressure	
	ECCS minimum high-pressure pump/accumulator and injection setpoint on primary coolant low pressure	
	ECCS minimum high-pressure pump/accumulator and injection setpoint on low flow	
	ECCS minimum high-pressure pump/accumulator and injection setpoint on pressurizer low level	
	ECCS maximum setpoint on sustained low flow time	
	ECCS maximum setpoint on containment high pressure	
	ECCS storage tank minimum temperature	piping integrity

Table B.2: Partial List of Limiting Events in Class 5 (cont.)

System/Component Failure of:	Limited Plant Parameters	Functional Requirements or Limiting Effects
boiler pressure control + shutdown system + single failure in the other shutdown system	shutdown procedure	heat sink
boiler inventory control + shutdown system + single failure in the other shutdown system	shutdown system boiler low-level trip setpoint	fuel sheath temperature
de-aerator inventory control + shutdown system + single failure in the other shutdown system	shutdown system boiler low-level trip setpoint	
	shutdown system boiler feed water pressure trip set point	
primary coolant pressure control + shutdown system + single failure in the other shutdown system	shutdown system primary coolant low-pressure trip setpoint	fuel sheath temperature
	shutdown system pressurizer low-level setpoint	
moderator inventory control + shutdown system + single failure in the other shutdown system	shutdown system high-neutron overpower trip setpoint	

...continued

Table B.2: Partial List of Limiting Events in Class 5 (cont.)

System/Component Failure of:	Limited Plant Parameters	Functional Requirements or Limiting Effects
primary pressure relief valve(s) + shutdown system + single failure in the other shutdown system	shutdown system pressurizer low level trip setpoint	fuel sheath temperature
	shutdown system primary coolant low pressure trip setpoint	
	ECCS (same as small LOCA)	
piping or calandria tube, causing a loss of moderator + shutdown system + single failure in the other shutdown system	shutdown system trip setpoint on moderator low level	fuel sheath temperature
piping, causing a small loss of reactor primary coolant + ECCS	coolant pump trip minimum time delay	fuel temperature
	coolant pump trip maximum pressure setpoint	
pressure relief valve in a vacuum containment system + piping, causing a small loss of reactor primary coolant ten or more hours later	manual ECCS procedure	heat sink

Table B.2: Partial List of Limiting Events in Class 5 (cont.)

System/Component Failure of:	Limited Plant Parameters	Functional Requirements or Limiting Effects
piping, causing a large loss of reactor primary coolant + shutdown system + single failure in the other shutdown system	maximum bundle power	fuel central temperature
	maximum moderator poison	
	maximum flux tilt	
	minimum shutdown system speed/pressure (redundant components operational, poison)	
	minimum fuel to shield plug gap	fuel axial expansion, strain, and temperature, and pressure tube temperature and strain
	minimum channel bearing length	pressure tube axial expansion, contraction and rolled joint pullout pressure tube axial expansion, contraction and rolled joint pullout
	extent of pressure tube flaws	pressure tube integrity
piping, causing a large loss of reactor primary coolant + containment system single failure	containment pressure relief valve minimum capacity	containment pressure
	dousing tank minimum level	
	dousing tank maximum temperature	
	containment system maximum pressure	
	containment system maximum temperature	
	ECCS storage tank maximum temperature	

...continued

Table B.2: Partial List of Limiting Events in Class 5 (cont.)

System/Component Failure of:	Limited Plant Parameters	Functional Requirements or Limiting Effects
piping, causing a large loss of reactor primary coolant + ECCS + Class IV power + moderator cover gas[3]	maximum moderator outlet temperature	calandria tube strain
piping, causing a large loss of reactor primary coolant + ECCS + containment system single failure	containment system auxiliary pressure relief valve minimum capacity	dose
	containment system filter minimum efficiency	
	containment system filter maximum desorption rate	
	ignitor locations	hydrogen concentration
	containment system cooling configuration	
flow (blockage) in any fuel channel assembly + shutdown system + ECCS + single failure in the other shutdown system	moderator heat sink capability	integrity
	moderator strength	
	moderator poison addition system minimum rate and capacity	reactivity
	moderator maximum boron concentration	
	shutdown system depth	
	shutdown system configuration and strength	
	reactor primary coolant maximum purity	
	emergency service water system to moderator system capacity	

Table B.2: Partial List of Limiting Events in Class 5 (cont.)

System/Component Failure of:	Limited Plant Parameters	Functional Requirements or Limiting Effects
piping, causing a large loss of reactor primary coolant + containment	ECCS storage tank minimum level during recovery	dose/backflow
piping, causing loss of secondary coolant + emergency service water system + residual heat removal system	heat sink	dose
piping, causing a large loss of reactor primary coolant + Class IV power + shutdown system + ECCS single failure	ECCS capacity	fuel sheath temperature
	ECCS injection valves opening time	
	ECCS high-pressure pump runup time	
	ECCS number of valves open	
	ECCS setpoint and opening time for high-pressure pump bypass valves	
	ECCS setpoint on minimum low injection pressure for the low-pressure pump recirculation valves to close	

...continued

Table B.2: Partial List of Limiting Events in Class 5 (cont.)

System/Component Failure of:	Limited Plant Parameters	Functional Requirements or Limiting Effects
*Turbine breakup by turbine generator load rejection + failure of turbine overspeed protection	emergency service water redundant pump auto start and minimum pressure	boiler level, containment system temperature, moderator system pressure, end shield cooling system pressure, and air conditioning
	layout and protection of safety systems, primary coolant system, moderator system, fuelling system, and fuel storage	shutdown, heat sink, and dose
*Drop of a large load on the reactivity mechanism deck	operational procedures	shutdown
*Failure of a boiler support	support design and inspection	integrity and containment
*Massive mechanical failure of a reactor-primary-coolant-pump component	inspection	shutdown, heat sink, and containment
*Massive (full length) failure of a reactor header	shutdown speed	fuel temperature
	ECCS connections	
*Massive failure of the station-service-water intake tunnel or discharge duct	emergency service water	flooding and heat sink

*Events of Extremely Low Probability — The consequences of these events are determined unless justification, subject to acceptance by the AECB, is given to demonstrate that their probability is sufficiently low

Table B.3: Partial List of Limiting Common Cause Events

Event	Limited Plant Parameters	Functional Requirements or Limiting Effects
fire in one fire area and flammable liquids	layout of systems	shutdown, heat sink, and monitoring
	safety design requirements	
earthquake	safety design requirements for containment, reactor building internal structure, liquid shutdown system, shutoff rods, primary coolant system, boilers, ECCS, emergency power, emergency service water, boiler emergency cooling, secondary control area	integrity, shutdown, heat sink, containment, and monitoring
	moderator and D_2O management maximum tritium concentration	dose
	emergency electrical power battery capacity	boiler level
	emergency electrical power generators capacity and maximum start time	
	emergency service water redundant pump auto start and minimum pressure	boiler level, containment system temperature, moderator system pressure, end shield cooling system pressure, and air conditioning
tornado	layout of systems	heat sink
	safety design requirements	integrity, building pressure relief, and containment
	emergency service water redundant pump auto start and minimum pressure	boiler level, containment system temperature, moderator system pressure, end shield cooling system pressure, and air conditioning

...continued

Table B.3: Partial List of Limiting Common Cause Events (cont.)

Event	Limited Plant Parameters	Functional Requirements or Limiting Effects
explosion or flammable gas clouds	emergency procedures	heat sink
	structural strength	
release of toxic gases	breathing equipment and procedures	habitability
release of corrosive chemicals	one group of safety system qualified	heat sink
internal flooding	protective structures	heat sink and containment
external flooding	layout of systems	heat sink
	safety design requirements	
extreme weather (wind, rain, hail, snow, ice, lightning, temperature, drought)	contingencies	
aircraft crash	site	integrity of containment and safety systems
electromagnetic interference from telecommunications equipment	shielding and procedures limiting the use of telecommunications equipment	correct functioning of safety and control systems

Notes

1. The list of limiting events and limited parameters may also be useful for deciding on site and construction licences.

2. The report "Application of Event Tables" by R.A. Brown and Associates Ltd. (report number 9703, May 30, 1997, available from the AECB as report RSP-51) shows additional event combination that are limiting events for various emergency procedures primarily related to shutting down and heat sinks.

3. The cover gas system is not credited for a large break unless protected and reliable. If the cover gas system were credited, the cover gas pressure could be increased instead of lowering the moderator outlet temperature. The thickness of the lower calandria tubes would also have to be increased so that they do not collapse when the increased cover gas pressure is added to the moderator water pressure.